IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ARLINGTON TECHNOLOGIES LLC,	§ § §	
Plaintiff,	§ § §	**JURY TRIAL DEMANDED**
v.	§ §	
T-MOBILE US, INC., T-MOBILE USA, INC., SPRINT LLC, SPRINT SOLUTIONS LLC, AND SPRINT SPECTRUM LLC	§ § § §	**C.A. NO. 2:25-cv-00279**
Defendants.	§ § §	

PLAINTIFF'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Arlington Technologies LLC ("ATL" or "Plaintiff") files this Complaint against Defendants T-Mobile US, Inc., T-Mobile USA, Inc., Sprint LLC, Sprint Solutions LLC, and Sprint Spectrum LLC (collectively, "T-Mobile" or "Defendant") for infringement of U.S. Patent No. 7,193,986 (the "'986 patent"), U.S. Patent No. 7,324,491 (the "'491 patent"), U.S. Patent No. 7,408,925 (the "'925 patent"), U.S. Patent No. 8,886,789 (the "'789 patent") and U.S. Patent No. 9,398,055 (the "'055 patent"), collectively, the "Asserted Patents."

THE PARTIES

1.   Arlington Technologies LLC is a Texas limited liability company, with a principal place of business in Allen, TX.

2.   On information and belief, Defendant T-Mobile US, Inc. is a corporation organized under the laws of the Delaware, with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006. T-Mobile US, Inc. may be served with process through its registered agent for service, Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

3.   On information and belief, Defendant T-Mobile USA, Inc. is a corporation organized under the laws of the Delaware, with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006. T-Mobile USA, Inc. is registered to conduct business in the State of Texas and has appointed Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701 as its agent for service of process.

4.   On information and belief, Defendant Sprint LLC ("Sprint") is a Delaware limited liability company with a principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006-1350.

5.   On information and belief, Defendant Sprint Solutions LLC ("Sprint Solutions") is a Delaware limited liability company with a principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006- 1350.

6.   On information and belief, Defendant Sprint Spectrum LLC ("Sprint Spectrum") is a Delaware limited liability company with a principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006-1350.

7.   Defendant operates one or more wireless telecommunications networks to provide wireless telecommunications products and services in the United States under brand names including, but not limited to, "T-Mobile" and "Sprint." On information and belief, Sprint was merged into T-Mobile in 2020 and T-Mobile, as the emerging company, assumed all liabilities for past, present, and future damages related to Sprint's infringement of the Asserted Patents.

8.   Defendant is an information technology company and develops and sells wireless telecommunications products and services. Defendant sells its products and services to customers, including customers in this District.

2

9.   Defendant operates and owns the t-mobile.com website, and it markets, offers, distributes, and provides technical support for its wireless telecommunications products and services throughout the United States including in this District.

10.   Defendant develops, designs, manufactures, distributes, markets, offers to sell, and/or sells infringing products and services within the United States, including in this District, and otherwise purposefully directs infringing activities to this District in connection with its Texas offices; its websites; and its other places of business in Texas and the rest of the United States. Defendant participates in the design, development, manufacture, sale for importation into the United States, offers for sale for importation into the United States, importation into the United States, sale within the United States after importation, and offers for sale within the United States after importation, of wireless telecommunications products and services that infringe the Asserted Patents.

11.   On information and belief, Defendant is engaged in making, using, selling, offering for sale, and/or importing, and/or inducing its subsidiaries, affiliates, retail partners, and customers in the making, using, selling, offering for sale, and/or importing throughout the United States, including within this District, the products, such as wireless telecommunications products and services, accused of infringement.

12.   Through offers to sell, sales, imports, distributions, and other related agreements to transfer ownership of Defendant's electronics, such as wireless telecommunications equipment, and/or Defendant's services, such as wireless telecommunications services, with distributors and customers operating in and maintaining a significant business presence in the U.S. and/or its U.S. subsidiaries Defendant does business in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

13.   This is an action for patent infringement arising under the patent laws of the United

States, 35 U.S.C. §§ 1, et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

14.   This Court has specific and general personal jurisdiction over Defendant consistent

with the requirements of the Due Process Clause of the United States Constitution and the Texas

Long Arm Statute because, inter alia, (i) Defendant has engaged in continuous, systematic, and

substantial business in Texas; (ii) Defendant is registered to do business in Texas; (iii) Defendant

maintains regular and established places of business in this District; (iv) Defendant has committed

and continues to commit, acts of patent infringement in this State and in this District. Such acts of

infringement include the making, using, testing, offering for sale, and selling of Accused Products

(as more particularly identified and described throughout this Complaint, below) that leverage and

infringe the inventions of the Asserted Patents in this State and this District and/or inducing others

to commit acts of patent infringement in this State and District.

15.   On information and belief, Defendant has purposefully and voluntarily placed, and

is continuing to place, one or more Accused Products into the stream of commerce through

established distribution channels (including the Internet) with the knowledge and intent that the

Accused Products are and/or will be used, sold to and purchased by consumers in the United States,

this State, and this District; and with the knowledge and expectation that the Accused Products

(whether in standalone form or as integrated in downstream products) will be imported into the

United States, this State, and this District.

16.   Defendant maintains a "regular and established" place of business in this District,

including by (a) maintaining or controlling retail stores in this District, (b) maintaining and

operating infringing base stations in this District, including on cellular towers and other installation sites owned or leased by them, and (c) maintaining and operating other places of business in this District, including those where research, development, or sales are conducted, where customer service is provided, or where repairs are made. Defendant's significant physical presence in this District includes, but not limited to, ownership of or control over property, inventory, or infrastructure. For example, Defendant maintains a corporate office in this District, located at 3560 Dallas Pkwy, Frisco, Texas 75034. Defendant also maintains numerous retail stores in this District through which it transacts business, including in Allen, Athens, Beaumont, Canton, Denton, Frisco, Kilgore, Longview, Marshall, McKinney, Nacogdoches, Texarkana, and Tyler, Texas. On information and belief, Defendant further maintains cellular base stations in this District that provide wireless telecommunications services to customers in this District, including on cellular towers and other installation sites owned or leased by Defendant.

17.   In addition, Defendant has derived substantial revenues from its infringing acts occurring within this State and this District. It has substantial business in this State and this District, including: (i) at least part of its infringing activities alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent conduct, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported, and services provided to Texas residents. Defendant derives benefits from its presence in this District, including, but not limited to, sales revenue and serving customers using its mobile network in this District. For example, Defendant receives revenue from its corporate stores in this District, by selling network access, phones/products, and services, and by receiving payment for network access, phones/products, and services. Defendant derives benefits from its presence in this District, including, but not limited

5

to, sales revenue and serving customers using its mobile network in this District. For example, Defendant receives revenue from its corporate stores in this District, by selling network services.

18.   In addition, Defendant has knowingly induced, and continue to knowingly induce, infringements within this State and this District by advertising, marketing, offering for sale and/or selling Accused Products (as more particularly identified and described throughout this Complaint) that incorporate the fundamental technologies covered by the Asserted Patents. Such advertising, marketing, offering for sale and/or selling of Accused Products is directed to consumers, customers, integrators, suppliers, distributors, resellers, partners, and/or end users, and this includes providing instructions, user manuals, advertising, and/or marketing materials that facilitate, direct and encourage use of infringing functionality with Defendant's knowledge thereof.

19.   Defendant has, thus, in the many ways described above, availed itself of the benefits and privileges of conducting business in this State and willingly subjected itself to the exercise of this Court's personal jurisdiction over it. Indeed, Defendant has sufficient minimum contacts with this forum through its transaction of substantial business in this State and this District and its commission of acts of patent infringement as alleged in this Complaint that are purposefully directed towards this State and District.

20.   Venue is proper in the Eastern District of Texas pursuant to 28 U.S.C. §§ 1391 and 1400(b) because, among other things, (i) Defendant is subject to personal jurisdiction in this District; (ii) Defendant has committed acts of patent infringement in this District; and (iii) Defendant has regular and established places of business in this District. On information and belief, Defendant maintains "regular and established" places of business in this District, including a corporate office in this District, located at 3560 Dallas Pkwy, Frisco, Texas 75034, and numerous

retail stores in this District through which it transacts business, including in Allen, Athens, Beaumont, Canton, Denton, Frisco, Kilgore, Longview, Marshall, McKinney, Nacogdoches, Texarkana, and Tyler, Texas.

21.   Moreover, on information and belief, Defendant has previously litigated patent infringement cases before this Court without contesting jurisdiction and venue.

DEFENDANT'S PRE-SUIT KNOWLEDGE OF ITS INFRINGEMENTS

22.   Prior to the filing of the Complaint, Plaintiff attempted to engage Defendant and/or its agents in good faith licensing discussions related to the Asserted Patents, including by sending them correspondence on February 10, 2025, notifying Defendant of the need to license the Asserted Patents. Defendant's past and continuing sales of its devices i) willfully infringe the Asserted Patents and ii) impermissibly take the significant benefits of Plaintiff's patented technologies without fair compensation to Plaintiff.

23.   The Accused Products addressed in the Counts below include, but are not limited to, products and services identified in ATL's letter to Defendant. Defendant's past and continuing sales of the Accused Products (i) willfully infringe the Asserted Patents and (ii) impermissibly usurp the significant benefits of ATL's patented technologies without fair compensation.

THE ASSERTED PATENTS AND TECHNOLOGY

24.   ATL is the sole and exclusive owner of all right, title, and interest in the Asserted Patents and holds the exclusive right to take all actions necessary to enforce its rights in, and to, the Asserted Patents, including the filing of this patent infringement lawsuit. Indeed, ATL owns all substantial rights in the Asserted Patents, including the right to exclude others and to recover damages for all past, present, and future infringements.

25.   The '986 patent is entitled, "Wireless network medium access control protocol." The '986 patent lawfully issued on March 20, 2007, and stems from U.S. Patent Application No. 10/158,680, which was filed on May 30, 2002.

26.   The '491 patent is entitled, "Method and apparatus for over-the-air bandwidth reservations in wireless networks." The '491 patent lawfully issued on January 29, 2008, and stems from U.S. Application No. 10/978,072, which was filed on October 28, 2004.

27.   The '925 patent is entitled, "Originator based directing and origination call processing features for external devices." The '925 patent lawfully issued on August 5, 2008, and stems from U.S. Application No. 10/846,984, which was filed on May 14, 2004.

28.   The '789 patent is entitled, "SIP monitoring and control anchor points." The '789 patent lawfully issued on November 11, 2014, and stems from U.S. Application No. 12/783,224, which was filed on May 19, 2010.

29.   The '055 patent is entitled, "Secure call indicator mechanism for enterprise networks." The '055 patent lawfully issued on July 19, 2016, and stems from U.S. Application No. 13/631,123, which was filed on September 28, 2012.

30.   The claims of the Asserted Patents are directed to patent-eligible subject matter under 35 U.S.C. § 101. They are not directed to an abstract idea, and the technologies covered by the claims comprise systems and/or ordered combinations of features and functions that, at the time of invention, were not, alone or in combination, well-understood, routine, or conventional.

31.   To the extent necessary, ATL has complied with the requirements of 35 U.S.C. § 287, such that ATL may recover pre-suit damages.

COUNT I
(INFRINGEMENT OF U.S. PATENT NO. 7,193,986)

32.   Plaintiff incorporates the preceding paragraphs herein by reference.

33.   This cause of action arises under the patent laws of the United States, and, in particular, 35 U.S.C. §§ 271, *et seq.*

34.   Plaintiff is the assignee of the '986 patent, with ownership of all substantial rights in the '986 patent, including the right to exclude others and to enforce, sue, and recover damages for past, present, and future infringements.

35.   The '986 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination.

36.   Defendant has and continues to directly and/or indirectly infringe (by inducing infringement and/or contributing to infringement) one or more claims of the '986 patent in this District and elsewhere in Texas and the United States.

37.   Defendant designs, develops, manufactures, assembles and markets wireless access points that are configured to support 802.11ax, such as the T-Mobile 5G Gateway G4AR, T-Mobile 5G Gateway G4SE, Sagemcom Fast 5688W Gateway, Arcadyan KVD21 Gateway, and Nokia 5G21 Gateway ("the '986 Accused Products").

38.   Defendant directly infringes the '986 patent under 35 U.S.C. § 271(a) by using, making, offering for sale, selling, and/or importing the '986 Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '986 patent.

39.   For example, Defendant infringes claim 1 of the '986 patent[1] via the '986 Accused Products. The '986 Accused Products comprise a "master wireless network device including a

---

[1] Throughout this Complaint, wherever ATL identifies specific claims of the Asserted Patents infringed by Defendant, ATL expressly reserves the right to identify additional claims, products and/or services in its infringement contentions in accordance with applicable local rules and the Court's case management order. Specifically identified claims throughout this Complaint are provided for notice pleading only.

wireless medium adaptor and a component implementing a medium access protocol." For example, the '986 Accused Products are wireless access points that support 802.11ax target wake time ("TWT") functionality.

Tech Specs

- Dimensions (W x H)
  - 228 (H) x 180 (W) x 76 (D) mm
- Weight
  - 880 g
  - 1.94 lbs
- Operating environment
  - 0° – 40° C (32° F – 104° F)
- IoT / GPS
  - Bluetooth 5.1
  - GPS
- Power adapter
  - AC
- Power input
  - 100 - 240V, 3A @ DC 15V, 50/60Hz
- Theoretical power consumption
  - 45 W
- Wi-Fi connectivity
  - 11ax 4x4 2.4G
  - 11ax 4x4 5G
  - Seamless roaming

Source: T-Mobile 5G Gateway (G4AR & G4SE) Tech Specs, https://www.t-mobile.com/support/home-internet/5g-gateway-g4ar.

40.   The '986 Accused Products are configured such that the component is "arranged to cause said adaptor to transmit temporally spaced packets of information." For example, the 802.11ax standard specifies that a TWT responding AP (i.e., a master wireless network device) will transmit frames (i.e., packets of information) during the TWT Service Period (SP) (i.e., temporally spaced):

10.47.1 TWT overview

Target wake times (TWTs) allow STAs to manage activity in the BSS by scheduling STAs to operate at different times in order to minimize contention and to reduce the required amount of time that a STA utilizing a power management mode needs to be awake. TWTs can be individual TWTs, which are described in 10.47 and 26.8.2, or broadcast TWTs, which are described in 26.8.3.

STAs that request a TWT agreement are called TWT requesting STAs and the STAs that respond to their requests are TWT responding STAs. A TWT requesting STA is assigned specific times to wake and exchange frames with the TWT responding STA. A TWT requesting STA communicates wake scheduling

10.47.4 Implicit TWT operation

The TWT values for an implicit TWT are periodic. A TWT requesting STA operating with an implicit TWT agreement shall determine the next TWT SP start time by adding the value of TWT Wake Interval associated with this TWT agreement to the value of the start time of the current TWT SP. A TWT requesting STA operating with an implicit TWT agreement with a TWT flow identifier that matches the TWT flow identifier of

41.   The '986 Accused Products are configured such that the component is "arranged to receive packets of information through said adaptor from slave network devices" with "at least some of said transmitted packets including a pointer indicating the relative time before which a designated packet of information will be transmitted" and "designated packet of information including an indication of the slave network devices participating in said network and respective indications as to when participating slave network devices should transmit packets of information for reception by said master wireless network device." For example, the 802.11ax standard specifies that a TWT scheduling AP can exchange frames at specific times and receive wake scheduling information (i.e., receive packets of information) from TWT requesting STAs (i.e., slave network devices):

10.47.1 TWT overview

Target wake times (TWTs) allow STAs to manage activity in the BSS by scheduling STAs to operate at different times in order to minimize contention and to reduce the required amount of time that a STA utilizing a power management mode needs to be awake. TWTs can be individual TWTs, which are described in 10.47 and 26.8.2, or broadcast TWTs, which are described in 26.8.3.

STAs that request a TWT agreement are called TWT requesting STAs and the STAs that respond to their requests are TWT responding STAs. A TWT requesting STA is assigned specific times to wake and exchange frames with the TWT responding STA. A TWT requesting STA communicates wake scheduling information to its TWT responding STA and the TWT responding STA devises a schedule and delivers TWT values to the TWT requesting STA when a TWT agreement has been established between them. When explicit TWT is employed, a TWT requesting STA wakes and performs a frame exchange and receives the next TWT information in a response from the TWT responding STA as described in 10.47.3. When implicit TWT is used, the TWT requesting STA calculates the Next TWT by adding a fixed value to the current TWT value as described in 10.47.4. STAs need not be made aware of the TWT values of other STAs. A TWT requesting STA and a TWT responding STA shall set the Negotiation Type subfield to 0 in the TWT element of transmitted frames containing the TWT element, except when the STAs are HE STAs. Additional TWT setup exchanges between HE STAs for individual TWT operation are defined in 26.8.

The 802.11ax standard further specifies that a TWT responding AP will include the start time for a series of TWT SPs (i.e., a pointer indicating the relative time) corresponding to a single Flow Identifier of an Implicit TWT agreement in the TWT field of the TWT element:

10.47.4 Implicit TWT operation

The TWT responding STA shall include the start time for a series of TWT SPs corresponding to a single TWT Flow Identifier of an Implicit TWT agreement in the Target Wake Time field of the TWT element which contains a value of Accept TWT in the TWT Setup Command field and the TWT Flow Identifier value corresponding to that TWT agreement in the TWT Flow Identifier subfield. The start time of the TWT SP series indicates the beginning time of the first TWT SP in the series. Subsequent TWT SPs start times are determined by adding the value of TWT Wake Interval to the current TWT SP start time.

9.4.1.60 TWT Information field

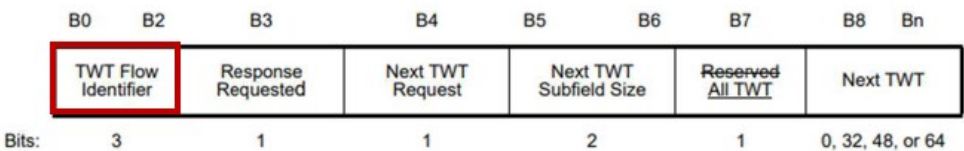| B0 B2	B3	B4	B5 B6	B7	B8 Bn
TWT Flow Identifier	Response Requested	Next TWT Request	Next TWT Subfield Size	Reserved All TWT	Next TWT
Bits: 3	1	1	2	1	0, 32, 48, or 64

Figure 9-142—TWT Information field format

The 802.11ax standard further specifies that a TWT scheduling AP will transmit a TWT element including a TWT Group Assignment field (i.e., indication of the slave network devices participating in said network) that indicates TWT Group Assignment of the slave network devices participating in the network:

9.4.2.199 TWT element

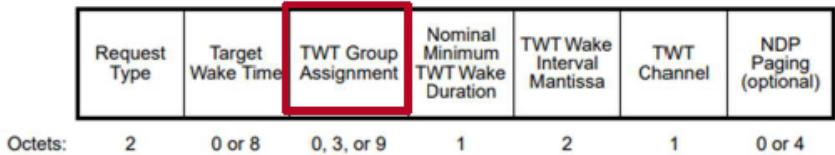| Request Type	Target Wake Time	TWT Group Assignment	Nominal Minimum TWT Wake Duration	TWT Wake Interval Mantissa	TWT Channel	NDP Paging (optional)
Octets: 2	0 or 8	0, 3, or 9	1	2	1	0 or 4

Figure 9-687a—Individual TWT Parameter Set field format

The TWT Group Assignment field provides information to a requesting STA about the TWT group to which the STA is assigned. This field contains the TWT Group ID, Zero Offset of Group (optional), TWT Unit, and TWT Offset subfields. The TWT Group Assignment field and the corresponding subfields are depicted in Figure 9-689.
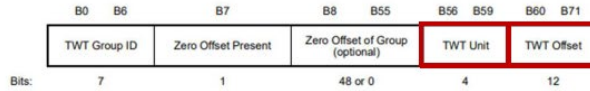
B0 B6	B7	B8 B55	B56 B59	B60 B71
TWT Group ID	Zero Offset Present	Zero Offset of Group (optional)	TWT Unit	TWT Offset
Bits: 7	1	48 or 0	4	12

Figure 9-689—TWT Group Assignment field format

The TWT Group ID subfield is an unsigned integer and indicates the identifier of the TWT group to which the requesting STA is assigned. A TWT group is a group of STAs that have TWT values that lie within a specific interval of TSF values. The value zero in the TWT Group ID subfield is used to indicate the unique TWT group, which contains all STAs in the BSS.

The 802.11ax standard further specifies that a TWT scheduling AP will transmit a TWT element including a TWT Group Assignment field. These include the TWT Unit and TWT Offset subfields that indicate the TWT Unit value used within the TWT group to calculate the TWT, and the position within the group when the STA should transmit, and thus the TWT positions of the other group members (i.e., when the participating slave network devices should transmit):

13

9.4.2.199 TWT element

The TWT Group Assignment field provides information to a requesting STA about the TWT group to which the STA is assigned. This field contains the TWT Group ID, Zero Offset of Group (optional), TWT Unit, and TWT Offset subfields. The TWT Group Assignment field and the corresponding subfields are depicted in Figure 9-689.

B0 B6	B7	B8 B55	B56 B59	B60 B71
TWT Group ID	Zero Offset Present	Zero Offset of Group (optional)	TWT Unit	TWT Offset

Bits: 7   1   48 or 0   4   12

Figure 9-689—TWT Group Assignment field format

The TWT Group ID subfield is an unsigned integer and indicates the identifier of the TWT group to which the requesting STA is assigned. A TWT group is a group of STAs that have TWT values that lie within a specific interval of TSF values. The value zero in the TWT Group ID subfield is used to indicate the unique TWT group, which contains all STAs in the BSS.

The TWT Unit subfield indicates the unit of increment of the TWT values within the TWT group identified by the TWT group ID. The TWT Unit subfield encoding is shown in Table 9-298.

Table 9-298—TWT Unit subfield encoding

TWT Unit subfield value	TWT Unit time value
0	32 µs
1	256 µs
2	1024 µs
3	8.192 ms
4	32.768 ms
5	262.144 ms
6	1.048576 s
7	8.388608 s
8	33.554432 s
9	268.435456 s
10	1073.741824 s
11	8589.934592 s
12–15	Reserved

The TWT Offset subfield indicates the position within the indicated group, of the STA corresponding to the RA of the frame containing the TWT element.

A non-AP STA uses the TWT Group ID, Zero Offset of Group, TWT Unit, and TWT Offset subfield values to compute its TWT value within the TWT group. A STA's TWT value is equal to the value of the Zero Offset of Group subfield plus TWT Offset subfield times the value of TWT Unit subfield.

42.   The technology discussion above and the exemplary '986 Accused Products provide context for Plaintiff's infringement allegations.

43.   At a minimum, Defendant has known of the '986 patent at least as early as the service of this complaint. Further, Defendant has known of the '986 patent at least as early as the filing date of the complaint. In addition, Defendant has known about the '986 patent since at least receiving correspondence from Plaintiff alerting Defendant to its infringement.

44.   On information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the '986 Accused Products that include or are made using all of the limitations of one or more claims of the '986 patent to directly infringe one or more claims of the '986 patent (e.g., claim 1, as discussed above) by using, offering for sale, selling, and/or importing the '986 Accused Products. Since at least the notice provided on the above-mentioned date, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '986 patent. Defendant intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia,

creating advertisements that promote the infringing use of the '986 Accused Products, creating

and/or maintaining established distribution channels for the '986 Accused Products into and within

the United States, manufacturing the '986 Accused Products in conformity with U.S. laws and

regulations, distributing or making available instructions or manuals for these products to

purchasers and prospective buyers, testing and certifying wireless networking features in the '986

Accused Products, and/or providing technical support, replacement parts, or services for these

products to these purchasers in the United States. For example, Defendant configures the '986

Accused Products to contain specific instructions, in the form of executable code and configuration

files, that cause such products to automatically implement and provide TWT functionality as

discussed above (i.e., Defendant provides instructions that cause end users to use '986 Accused

Products in an infringing manner). Moreover, in addition to the foregoing, Defendant encourages

its customers and end users to use the '986 Accused Products as wireless gateways according to

the 802.11ax standard and thus to use the '986 Accused Products in an infringing manner (e.g.,

through the implementation and use of TWT functionality).

Tech Specs

- Dimensions (W x H)
  - 228 (H) x 180 (W) x 76 (D) mm
- Weight
  - 880 g
  - 1.94 lbs
- Operating environment
  - 0° – 40° C (32° F – 104° F)
- IoT / GPS
  - Bluetooth 5.1
  - GPS
- Power adapter
  - AC
- Power input
  - 100 - 240V, 3A @ DC 15V, 50/60Hz
- Theoretical power consumption
  - 45 W
- Wi-Fi connectivity
  - 11ax 4x4 2.4G
  - 11ax 4x4 5G
  - Seamless roaming

Source: T-Mobile 5G Gateway (G4AR & G4SE) Tech Specs, https://www.t-mobile.com/support/home-internet/5g-gateway-g4ar.

45.   In the alternative, on information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '986 patent. For example, Defendant contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the '986 Accused Products. To the extent that the '986 Accused Products do not directly infringe one or more claims of the '986 patent, such products contain instructions, such as source code, that are especially adapted to cause the '986 Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the '986 Accused Products to conduct the 802.11 TWT protocol in an infringing manner and are a material part of the invention of the '986 patent and are not a staple article of commerce suitable for substantial non-infringing use.

46.   On information and belief, despite having knowledge of the '986 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '986 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Defendant's infringing activities relative to the '986 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

47.   Plaintiff has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Plaintiff in an amount that adequately compensates Plaintiff for Defendant's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II
(INFRINGEMENT OF U.S. PATENT NO. 7,324,491)

48.   Plaintiff incorporates the preceding paragraphs herein by reference.

49.   This cause of action arises under the patent laws of the United States, and, in particular, 35 U.S.C. §§ 271, *et seq*.

50.   Plaintiff is the assignee of the '491 patent, with ownership of all substantial rights in the '491 patent, including the right to exclude others and to enforce, sue, and recover damages for past, present, and future infringements.

51.   The '491 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination.

52.   Defendant has and continues to directly and/or indirectly infringe (by inducing infringement and/or contributing to infringement) one or more claims of the '491 patent in this District and elsewhere in Texas and the United States.

53.   Defendant designs, develops, manufactures, assembles and markets wireless access points that are configured to support Wi-Fi multimedia ("WMM"), such as the KVD21 Router, WE620443-T0 Wi-Fi Mesh Access Point, TMO-G4AR Router, TM-G5240 Router, TMUS-SUP-1 SYNCUP PETS tracker, and TMUS-SKW-2 SyncUP Kids Watch ("the '491 Accused Products").

54.   Defendant directly infringes the '491 patent under 35 U.S.C. § 271(a) by using, making, offering for sale, selling, and/or importing the '491 Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '491 patent.

55.   For example, Defendant infringes claim 1 of the '491 patent via the '491 Accused Products. The '491 Accused Products support WMM:

Source: https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc#advanced_ filters.

The '491 Accused Products perform a method for "controlling access to a wireless network providing communication for a plurality of wireless traffic streams to assure quality of service for designated traffic" via their use of WMM. For example, the WMM specification outlines a method for controlling access to a wireless network for to assure QoS for designated traffic:

19

1.0 Overview

This document defines the specification for WMM, an 802.11 QoS implementation based on a subset of the draft IEEE 802.11e standard supplement [2]. It was originally motivated by the need to prevent market fragmentation caused by multiple, non-interoperable pre-standard subsets of the draft 802.11e standard that would otherwise occur. Deployment of WMM will deliver useful QoS functionality for services such as voice over 802.11 and streaming media.

1.3 WMM Features

3.   WMM will use an EDCA mechanism only, and except where explicitly indicated otherwise in this specification other 802.11 QoS features, including HCCA polling and associated signaling, Block Acknowledgement, and direct-link traffic, were not included in WMM.

4.3.10 QoS BSS

The first mechanism, designated the *enhanced distributed channel access* (EDCA), delivers traffic based on differentiating user priorities (UPs). This differentiation is achieved by varying the following for different UP values:

  —   Amount of time a STA senses the channel to be idle before backoff or transmission, or

  —   The length of the contention window to be used for the backoff, or

  —   The duration a STA transmits after it acquires the channel.

These transmissions might also be subject to certain channel access restrictions in the form of admission control. A DMG STA uses EDCA only within a contention based access period (CBAP). Details of EDCA are provided in 10.22.2 and, for DMG STAs, additional details are provided in 10.36.4, 10.36.5, and 10.36.6.3.

IEEE Std 802.11™-2016

---

56.   The '491 Accused Products assign "all communication of the designated traffic to use one of a plurality of priorities on the wireless network." For example, the '491 Accused Products assign designated traffic differentiating Access Categories (i.e., a plurality of priorities):

3.3 Assignment of Frames to Queues

3.3.1 Mappings for Unicast Frames

The MAC data service at a STA or AP provides for connectionless, asynchronous transport of MSDUs. Each MSDU transfer request includes an 802.1D Priority field equal to that value. The priority bits of the 802.1D field are mapped to Access Category (AC) according to Table 14 and are listed in increasing priority order. The UP field is carried in the QoS control field of an MPDU. The UP field references the AC the MPDU is transmitted at using the mapping defined in Table 14. At the receiver, the UP field carried in the MPDU shall be used to re-create the 802.1D priority information of the MSDU.

Table 14 802.1D Priority to AC mappings

Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation
lowest	1	BK	AC_BK	Background
	2	-		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
highest	7	NC		

Transmit frames are then placed in queues according to AC. The AP and STA may implement more queues for internal prioritization. Data frames with no priority information are treated as best effort.

57.   The '491 Accused Products require "that ones of the plurality of wireless traffic streams wanting to communicate using the one of the plurality of priorities and higher ones of the plurality of priorities and using a distributed medium access protocol submit bandwidth reservation requests to a wireless access point." For example, the '491 Accused Products require that when a client station ("STA") seeks to communicate using a specific access category (AC) corresponding to a user priority (i.e., a higher one of the plurality of priorities) using the EDCA mechanism (i.e., a distributed medium access protocol) must submit a WMM TSPEC element in an ADDTS request management frame:

3.5.3 Procedure at STAs

At any point, following association, the STA may decide, to explicitly request admission of traffic to be transmitted or/and received on a specific AC. The STA shall use the mappings in Table 14 to identify the sending AC from the UP field

In order to make such a request, the STA shall transmit a WMM TSPEC element contained in a ADDTS request management action frame with the following fields specified (i.e. non-zero): Nominal MSDU Size, Mean Data Rate, Minimum PHY Rate, and Surplus Bandwidth Allowance. The Medium Time field is not used in the request frame and shall be set to zero.

1.2 Terms and Definitions

Name	Definition
AC	Access category: A label for the common set of enhanced distributed channel access (EDCA) parameters that are used by a WMM STA to contend for the channel in order to transmit MSDUs with certain priorities. WMM defines 4 ACs.

enhanced distributed channel access (EDCA): The prioritized carrier sense multiple access with collision avoidance (CSMA/CA) access mechanism used by quality-of-service (QoS) stations (STAs) in a QoS basic service set (BSS) and STAs operating outside the context of a BSS. This access mechanism is also used by the QoS access point (AP) and operates concurrently with hybrid coordination function (HCF) controlled channel access (HCCA).

58.　　　The '491 Accused Products receive "a bandwidth reservation by one of the plurality of wireless traffic streams for communication from the wireless access point in response to a bandwidth reservation request upon bandwidth being available on the wireless network." For example, the '491 Accused Products assign a bandwidth reservation to a traffic stream in an ADDTS response management action frame from the access point upon bandwidth being available:

3.5.2 Procedures at the AP

The AP shall respond to requests for admission conveyed in the WMM TSPEC request elements for those AC(s) with ACM flag set to 1. If the AP supports delivery-enabled-only or trigger-enabled-only U-APSD operation it shall respond to requests for admission conveyed in the WMM TSPEC request elements even if the ACM flag is set to 0. If the ACM flag is set to 0 for an AC,

the AP is not required to respond to a TSPEC request on that AC if the AP only supports bi-directional U-APSD settings (does not support delivery-enabled only or trigger-enabled only state). On receipt of a WMM TSPEC request element conveyed in an ADDTS Request Frame from an associated STA, the AP shall make a determination as to whether to

    a) accept the request

    b) deny the request

The AP may use any algorithm in making such a determination. If the AP decides to accept the request, the AP shall also derive the Medium Time from the information conveyed in the WMM TSPEC request element. The AP may use any algorithm in deriving the Medium Time, but normally it will use the procedure described in the Annex. Having made such a determination, the AP shall transmit a WMM TSPEC element to the requesting STA contained in a ADDTS response management action frame. If the AP is accepting the request, the Medium Time field shall be specified. An AP shall return a Medium Time equal to zero when accepting a unidirectional, downlink TS request.

59.   The '491 Accused Products communicate "by other ones of the plurality of wireless traffic streams using lower ones of the plurality of priorities without requiring bandwidth reservation requests." For example, the '491 Accused Products communicate traffic that does not need a specific AC (i.e., lower ones of the plurality of priorities) using, for example, a channel access time with a backoff function timer that does not require a bandwidth reservation request:

3.4 Channel Access Protocol

3.4.1 Reference Implementation

Subject to the conditions described in section 3.5.3, traffic for an admitted stream may be transmitted by using the parameters (AIFSN, TXOP Limit, CWmin, CWmax) of a lower-priority AC not configured for mandatory admission control without changing the user priority carried in the QoS control field of the frame. In this situation all references to these parameters in this section (3.4) shall be construed as references to those of the lower-priority AC.

3.4.3 Obtaining an EDCA TXOP

Each channel access timer shall maintain a backoff function timer, which has a value measured in backoff slots.

The duration AIFS[AC] is a duration derived from the value AIFSN[AC] by the relation

AIFS[AC] = AIFSN[AC] × aSlotTime + aSIFSTime

An EDCA TXOP is granted to a channel access function when the channel access function determines that it shall initiate the transmission of a frame exchange sequence. Transmission initiation shall be determined according to the following rules:

On specific slot boundaries, each channel access function shall make a determination to perform one and only one of the following functions:

    a) Initiate the transmission of a frame exchange sequence for that access function

    b) Decrement the backoff timer for that access function

    c) Invoke the backoff procedure due to an internal collision

    d) Do nothing for that access function.

1.2 Terms and Definitions

| Admitted AC	Traffic transmitted using an AC based on parameters in a WMM TSPEC element contained in an ADDTS response management action frame
Un-admitted AC	Traffic transmitted using an AC that did not require admission.

2.2.11 WMM TSPEC Element

A WMM TSPEC request shall be transmitted by a STA to an AP in order to request admission for an AC that requires admission control. The STA may transmit unadmitted traffic for those ACs for which the AP does not mandate admission control. A STA may need to transmit a WMM TSPEC request for an AC that does not mandate admission control, e.g for the establishment of the triggered power save mode of operation.

60.   The technology discussion above and the exemplary '491 Accused Products provide context for Plaintiff's infringement allegations.

61.   At a minimum, Defendant has known of the '491 patent at least as early as the service of this complaint. Further, Defendant has known of the '491 patent at least as early as the filing date of the complaint. In addition, Defendant has known about the '491 patent since at least receiving correspondence from Plaintiff alerting Defendant to its infringement.

62.   On information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the '491 Accused Products that include or are made using all of the limitations of one or more claims of the '491 patent to directly infringe one or more claims of the '491 patent (e.g., claim 1, as discussed above) by using, offering for sale, selling, and/or importing the '491 Accused Products. Since at least the notice provided on the above-mentioned date, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '491 patent. Defendant intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the '491 Accused Products, creating and/or maintaining established distribution channels for the '491 Accused Products into and within the United States, manufacturing the '491 Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying wireless networking features in the '491 Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States. For example, Defendant configures the '491

Accused Products to contain specific instructions, in the form of executable code and configuration files, that cause such products to automatically implement and provide WMM functionality as discussed above (i.e., Defendant provides instructions that cause end users to use Accused Products in an infringing manner). Moreover, in addition to the foregoing, Defendant encourages its customers and end users to use the '491 Accused Products according to the WMM standard and thus to use Accused Products in an infringing manner by having the Wi-Fi Alliance certify and advertise that the Accused Products comply with the WMM standard.
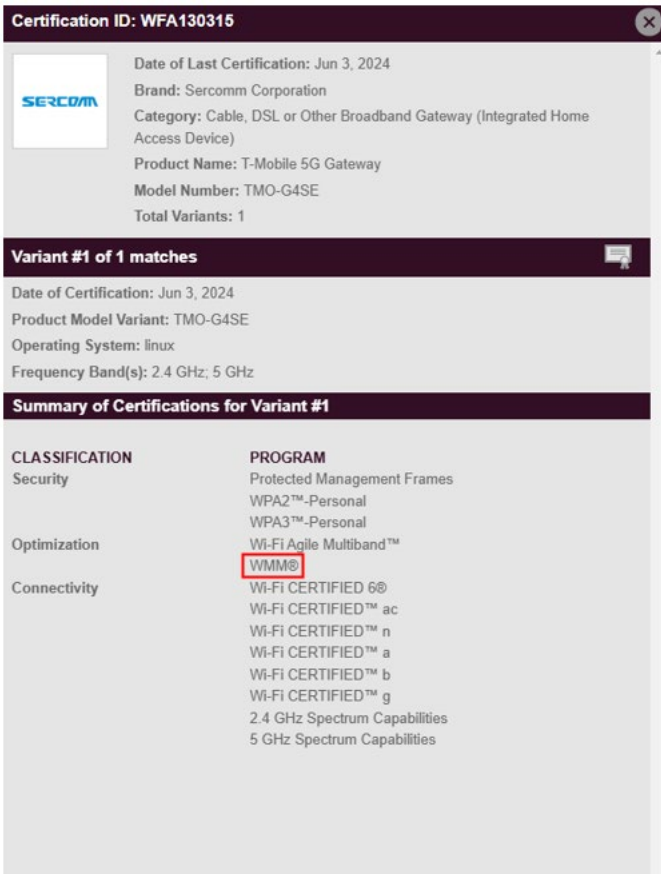
Source: https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc# advanced_ filters.

63.   In the alternative, on information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '491 patent. For example, Defendant contributes to the

direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the '491 Accused Products. To the extent that the '491 Accused Products do not directly infringe one or more claims of the '491 patent, such products contain instructions, such as source code, that are especially adapted to cause the '491 Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the '491 Accused Products to conduct the WMM QoS implementation in an infringing manner and are a material part of the invention of the '491 patent and are not a staple article of commerce suitable for substantial non-infringing use.

64.   On information and belief, despite having knowledge of the '491 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '491 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Defendant's infringing activities relative to the '491 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

65.   Plaintiff has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Plaintiff in an amount that adequately compensates Plaintiff for Defendant's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III
(INFRINGEMENT OF U.S. PATENT NO. 7,408,925)

66.   Plaintiff incorporates the preceding paragraphs herein by reference.

67.   This cause of action arises under the patent laws of the United States, and, in particular, 35 U.S.C. §§ 271, *et seq.*

68.   Plaintiff is the assignee of the '925 patent, with ownership of all substantial rights in the '925 patent, including the right to exclude others and to enforce, sue, and recover damages for past, present, and future infringements.

69.   The '925 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination.

70.   Defendant has and continues to directly and/or indirectly infringe (by inducing infringement and/or contributing to infringement) one or more claims of the '925 patent in this District and elsewhere in Texas and the United States.

71.   Defendant designs, offers for sale, uses, and sells services, such as Voice over LTE (VoLTE) in its cellular services ("the '925 Accused Products"), that infringe the '925 patent.

72.   Defendant directly infringes the '925 patent under 35 U.S.C. § 271(a) by using, making, offering for sale, selling, and/or importing the '925 Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '925 patent.

73.   For example, Defendant infringes claim 1 of the '925 patent via the '925 Accused Products. The '925 Accused Products utilize IMS mobile core services to provide VoLTE to its customers:
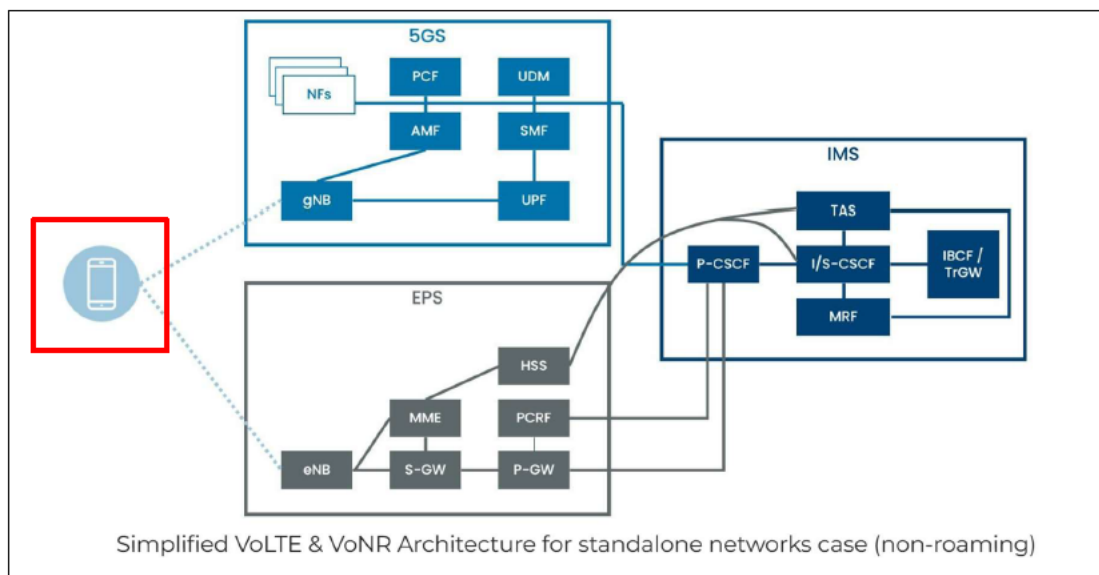

4G LTE

- Our 4G LTE network supplements our 5G network with coverage for 99% of Americans nationwide.
- VoLTE allows you to make and receive calls while connected to the LTE data network. It's available nationwide.
- HD Voice improves in-call voice quality for compatible phones on VoLTE.
- Enhanced Voice Services (EVS) is another codec for HD Voice that further enhances call quality.

Source: https://www.t-mobile.com/support/coverage/t-mobile-network.

> In fact, one of Mavenir's biggest customers is T-Mobile, which uses Mavenir for its IMS mobile core services including voice, video and messaging.

Source: https://www.fierce-network.com/wireless/mavenir-does-many-same-things-ericsson-nokia.

74.   The '925 Accused Products perform a "method for setting up a communication between first and second communication devices, the first communication device corresponding to a first directing server and first communication manager separate from the first directing server." For example, the '925 Accused Products set up a communication between a first communication device on the T-Mobile network and a second communication device. The communication may be, as one example, a voice call between the first and second communication devices:

Simplified VoLTE & VoNR Architecture for standalone networks case (non-roaming)

Source: https://www.3gpp.org/technologies/volte-vonr.

As part of this process, the Proxy Call Session Control Function ("P-CSCF") and Serving Call Session Control Function ("S-CSCF") both correspond to the first communication device as configured and registered between the first communication device and the IMS network:

> ### 5.1.1   Procedures related to Proxy-CSCF discovery
>
> #### 5.1.1.0   General
>
> The Proxy-CSCF discovery shall be performed using one of the following mechanisms:
>
> - As part of the establishment of connectivity towards the IP-Connectivity Access Network, if the IP-Connectivity Access Network provides such means.
>
> - Alternatively, the P-CSCF discovery may be performed after the IP connectivity has been established. To enable P-CSCF discovery after the establishment of IP connectivity, the IP-Connectivity Access Network shall provide the following P-CSCF discovery option to the UE:
>
>   - Use of DHCP to provide the UE with the domain name and/or IP address of a Proxy-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the Proxy-CSCF name, as described below in clause 5.1.1.1.
>
>   - The UE may be configured (e.g. during initial provisioning or via a 3GPP IMS Management Object (MO), TS 24.167 [64] or in the ISIM, TS 31.103 [69]) to know the fully qualified domain name (FQDN) of the P-CSCF or its IP address. If the domain name is known, DNS resolution is used to obtain the IP address.
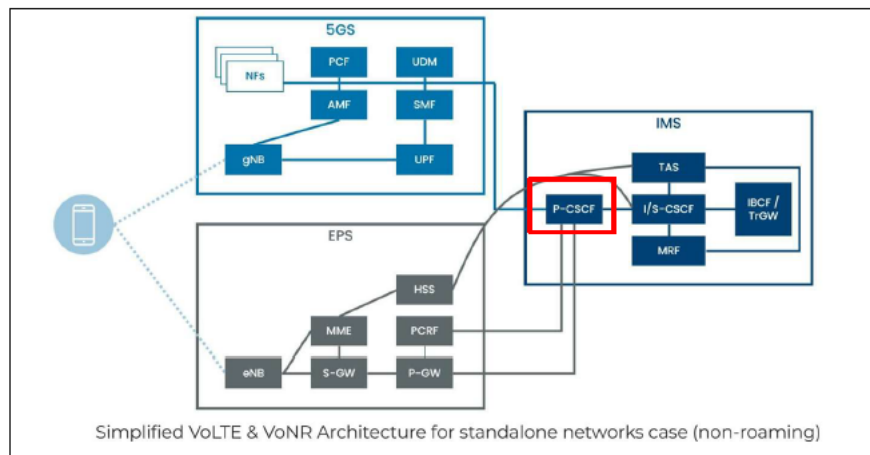>
> ### 5.1.2   Procedures related to Serving-CSCF assignment
>
> #### 5.1.2.1   Assigning a Serving-CSCF for a user
>
> When a UE attaches and makes itself available for access to IMS services by explicitly registering in the IMS, a S-CSCF shall be assigned to serve the UE.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.

75.   The '925 Accused Products cause "the first directing server receiving a call set up message at least one of addressed to and originated by the first communication device." For example, the communication set up process begins when the P-CSCF receives a SIP INVITE message from the first communication device, as a user initiates a voice call at the first communication device:

Simplified VoLTE & VoNR Architecture for standalone networks case (non-roaming)

Source: https://www.3gpp.org/technologies/volte-vonr.

A hosted PBX service will make use of SIP in order to connect VoIP endpoints such as a VoIP telephones or apps on a mobile device. Any business will have its PBX use SIP trunks in order to make a VoIP connection.

Source: https://www.telco-data.com/blog/sip-voip-pbx/.

4.6.1   Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs using the mechanism described in the clause "Procedures related to Local CSCF Discovery". The P-CSCF behaves like a Proxy (as defined in IETF RFC 3261 [12] or subsequent versions), i.e. it accepts requests and services them internally or forwards them on. The P-CSCF shall not modify the Request URI in the SIP INVITE message. The P-CSCF may behave as a User Agent (as defined in the IETF RFC 3261 [12] or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.
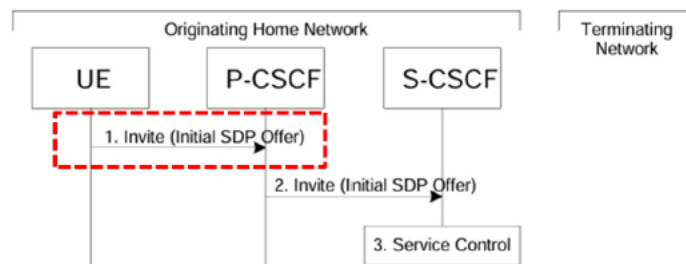
The call set up message is a SIP INVITE message, as signaling in a VoLTE call is performed using the SIP protocol:

5.6.2   (MO#2) Mobile origination, home

This origination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure described in clause 5.1.1. During registration, the home network allocates an S-CSCF in the home network.

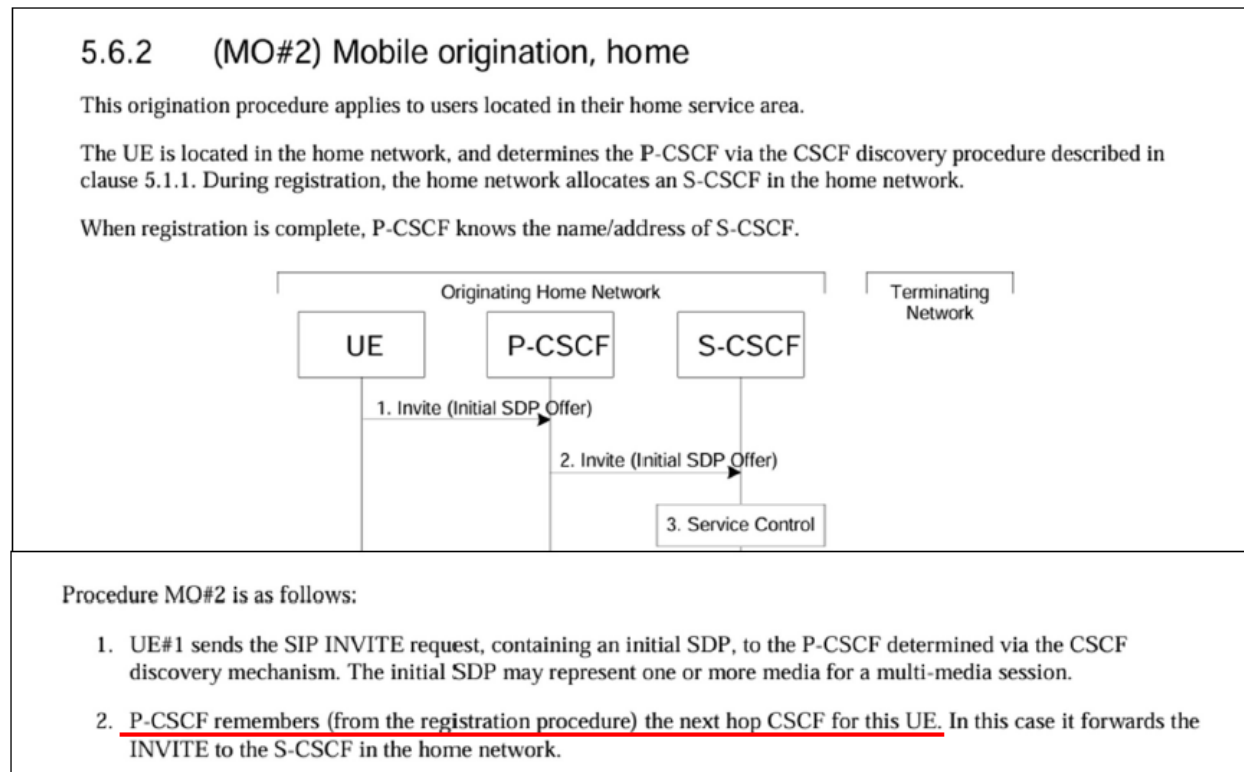When registration is complete, P-CSCF knows the name/address of S-CSCF.

Procedure MO#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. In this case it forwards the INVITE to the S-CSCF in the home network.

30

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.

76.   The '925 Accused Products cause "the first directing server determining that the first communication device has a corresponding first communication manager." For example, the P-CSCF will identify the first communication device and determine the S-CSCF that corresponds to the first communication device.

5.6.2   (MO#2) Mobile origination, home

This origination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure described in clause 5.1.1. During registration, the home network allocates an S-CSCF in the home network.

When registration is complete, P-CSCF knows the name/address of S-CSCF.

Procedure MO#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. In this case it forwards the INVITE to the S-CSCF in the home network.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.
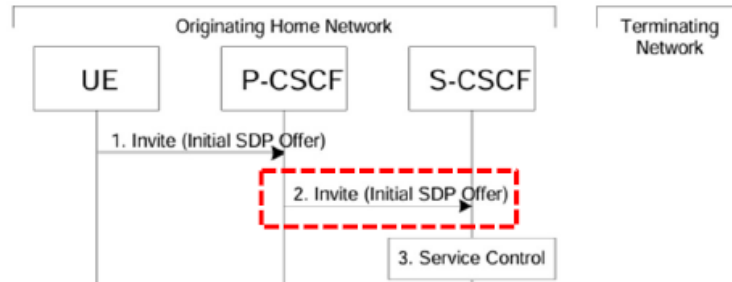
77.   The '925 Accused Products cause "the first directing server forwarding the call set up message to the first communication manager and requesting the first communication manager to perform at least one of call originating and terminating processing, the call setup message including a message in a route header of an INVITE message, the route header specifying the at least one of call originating and terminating processing." For example, the P-CSCF will forward the call set up message to the S-CSCF for voice call processing:

5.6.2   (MO#2) Mobile origination, home

This origination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure described in clause 5.1.1. During registration, the home network allocates an S-CSCF in the home network.

When registration is complete, P-CSCF knows the name/address of S-CSCF.

Procedure MO#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session.

2. P-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. In this case it forwards the INVITE to the S-CSCF in the home network.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.

The call set up message is routed to the S-CSCF according to the topmost ROUTE header in the call setup message. The S-CSCF will look for an "orig" parameter, or other designated information, in the ROUTE header field, which indicates a request for call originating processing. If no such parameter or designated information is present in the ROUTE header field, then call terminating processing is indicated:

5.4.3   General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1   Determination of UE-originated or UE-terminated case

Upon receipt of an initial request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the UE-originating case as described in subclause 5.4.3.2 if the request makes use of the information for UE-originating calls, which was added to the Service-Route header field entry of the S-CSCF during registration (see subclause 5.4.1.2.2F), e.g. the message is received at a certain port or the topmost Route header field contains a specific user part or parameter; or,

- perform the procedures for the UE-originating case as described in subclause 5.4.3.2 if the topmost Route header field of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header field; or,

- perform the procedures for the UE-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

Source: https://www.etsi.org/deliver/etsi_ts/124200_124299/124229/17.10.00_60/ts_
124229v171000p.pdf.

78.   The '925 Accused Products cause "the first communication manager performing the at least one of call originating and terminating processing." For example, the S-CSCF performs the call processing according to the services requested by the P-CSCF. If the second communication device is also a T-Mobile customer device, the call processing will include forwarding the setup message to an interrogating call session control function ("I-CSCF") within the IMS network:

4.6.3   Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

- For an originating endpoint (i.e. the originating user/UE, or originating AS)

  - Obtain from a database the Address of the entry point for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and forward the SIP request or response to that entry point.

    If a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity encapsulated in the P-GRUU or associated with the T-GRUU belongs to the same service profile.

  - When the destination name of the destination user (e.g. dialled phone number or SIP URI), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.

  - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

  - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.

  - Ensure the originating end point is subscribed to the determined IMS communication service.

  - Ensure that the content of the SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the originating endpoint matches the determined IMS communication service definition, based on originating user's subscription.

  - When the INVITE message includes an MPS code or an MPS input string, forward the INVITE, including the Service User's priority level if available.

  - When an MPS user is authorized by an AS for priority service, include the Service User's priority level received from the AS in the INVITE and forward the INVITE.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.

The S-CSCF performs the call processing according to the services requested by the P-CSCF.

5.5.2   (S-S#2) Single network operator performing origination and termination

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines that it belongs to a subscriber of the same operator. The request is therefore forwarded to a local I-CSCF. The I-CSCF queries the HSS for current location information, and finds the user either located in the home service area, or roaming. The I-CSCF therefore forwards the request to the S-CSCF serving the destination user.

Procedure S-S#2 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.

2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt

3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. Since it is local, the request is passed to a local I-CSCF.

4. I-CSCF shall query the HSS for current location information.

5. HSS responds with the address of the current Serving-CSCF for the terminating user.

6. I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt

8. The sequence continues with the message flows determined by the termination procedure.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

The S-CSCF performs call terminating processing if the second communication device is also a T-Mobile subscribed in the same network.

4.6.3   Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

- For a destination endpoint (i.e. the terminating user/UE)

  - Forward the SIP request or response to a P-CSCF.

  - Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, if the user is to receive the incoming session via the CS domain.

  - Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.

  - Ensure the terminating end point is subscribed to the determined IMS communication service.

  - Ensure that the content of SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the destination end point matches the determined IMS communication service definition, based on terminating user's subscription.

  - If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in IETF RFC 3312 [41].

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_
123228v140700p.pdf.

79.   The '925 Accused Products cause "the first directing server directing the call set up message to a destination referenced in the call set up message." For example, after the S-CSCF returns the call set up message to the P-CSCF, the P-CSCF forwards the message along to a destination address for the second communication device:

5.7.2   (MT#2) Mobile termination, home

This termination procedure applies to users located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedures described in clause 5.1.1.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.
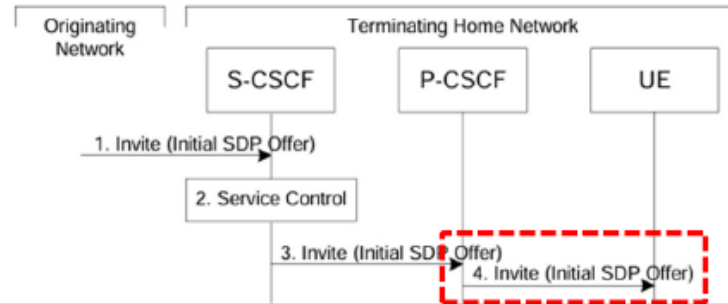
Procedure MT#2 is as follows:

1. UE#1 sends the SIP INVITE request, containing an initial SDP, via one of the origination procedures, and via one of the Serving to Serving-CSCF procedures, to the Serving-CSCF for the terminating user.

2. S-CSCF validates the service profile, and invokes any termination service logic required for this user. This includes authorization of the requested SDP based on the user's subscription for multi-media services.

3. S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF in the home network.

4. If the P-CSCF determines that the termination is for an MPS session, the P-CSCF derives the session information and invokes dynamic policy sending the derived session information to the PCRF. The P-CSCF remembers (from the registration procedure) the UE address, and forwards the INVITE to the UE.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_
123228v140700p.pdf.

80.   The technology discussion above and the exemplary '925 Accused Products provide context for Plaintiff's infringement allegations.

81.   At a minimum, Defendant has known of the '925 patent at least as early as the service of this complaint. Further, Defendant has known of the '925 patent at least as early as the filing date of the complaint. In addition, Defendant has known about the '925 patent since at least receiving correspondence from Plaintiff alerting Defendant to its infringement.

82.   On information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has actively induced, under U.S.C. § 271(b), its

distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the '925 Accused Products that include or are made using all of the limitations of one or more claims of the '925 patent to directly infringe one or more claims of the '925 patent (e.g., claim 1, as discussed above) by using, offering for sale, selling, and/or importing the '925 Accused Products. Since at least the notice provided on the above-mentioned date, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '925 patent. Defendant intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the '925 Accused Products, creating and/or maintaining established distribution channels for the '925 Accused Products into and within the United States, manufacturing the '925 Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, and testing the '925 Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States. For example, Defendant configures the '925 Accused Products to contain specific instructions, in the form of executable code and configuration files, that cause such products to automatically implement and provide VoLTE as discussed above (i.e., Defendant provides instructions that cause end users to use '925 Accused Products in an infringing manner). Moreover, in addition to the foregoing, Defendant encourages its customers and end users to use VoLTE communications that cause the '925 Accused Products to operate an infringing manner.

83.   In the alternative, on information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '925 patent. For example, Defendant contributes to the

direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the '925 Accused Products. To the extent that the '925 Accused Products do not directly infringe one or more claims of the '925 patent, such products contain instructions, such as source code, that are especially adapted to cause the '925 Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the '925 Accused Products to provide call control in an infringing manner and are a material part of the invention of the '925 patent and are not a staple article of commerce suitable for substantial non-infringing use.

84.   On information and belief, despite having knowledge of the '925 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '925 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Defendant's infringing activities relative to the '925 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

85.   Plaintiff has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Plaintiff in an amount that adequately compensates Plaintiff for Defendant's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV
(INFRINGEMENT OF U.S. PATENT NO. 8,886,789)

86.   Plaintiff incorporates the preceding paragraphs herein by reference.

87.   This cause of action arises under the patent laws of the United States, and, in particular, 35 U.S.C. §§ 271, *et seq*.

88.   Plaintiff is the assignee of the '789 patent, with ownership of all substantial rights in the '789 patent, including the right to exclude others and to enforce, sue, and recover damages for past, present, and future infringements.

89.   The '789 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code, after a full and fair examination.

90.   Defendant has and continues to directly and/or indirectly infringe (by inducing infringement and/or contributing to infringement) one or more claims of the '789 patent in this District and elsewhere in Texas and the United States.

91.   Defendant designs, offers for sale, uses, and sells services, such as Voice over LTE (VoLTE) in its cellular services ("the '789 Accused Products"), that infringe the '789 patent.

92.   Defendant directly infringes the '789 patent under 35 U.S.C. § 271(a) by using, making, offering for sale, selling, and/or importing the '789 Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '789 patent.

93.   For example, Defendant infringes claim 1 of the '789 patent via the '789 Accused Products. The '789 Accused Products utilize IMS mobile core services to provide VoLTE to its customers:
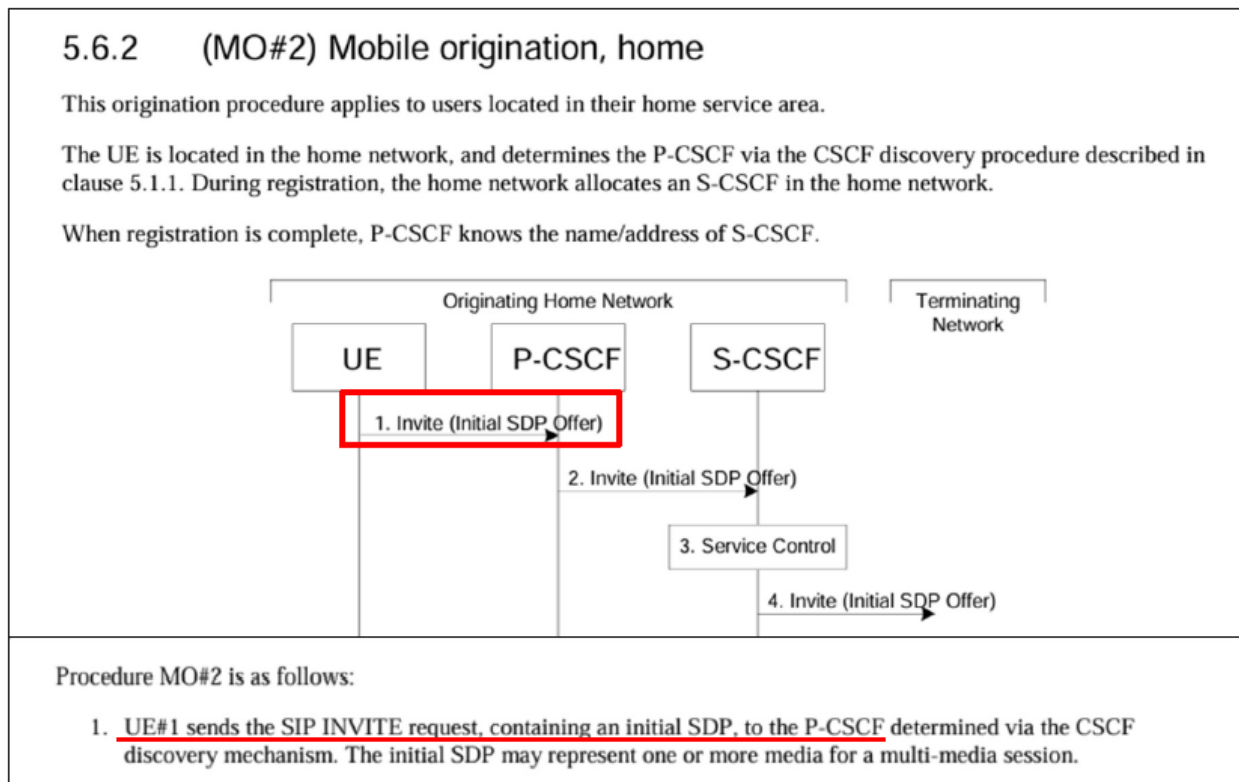

4G LTE

- Our 4G LTE network supplements our 5G network with coverage for 99% of Americans nationwide.
- VoLTE allows you to make and receive calls while connected to the LTE data network. It's available nationwide.
- HD Voice improves in-call voice quality for compatible phones on VoLTE.
- Enhanced Voice Services (EVS) is another codec for HD Voice that further enhances call quality.

Source: https://www.t-mobile.com/support/coverage/t-mobile-network.

> In fact, one of Mavenir's biggest customers is T-Mobile, which uses Mavenir for its IMS mobile core services including voice, video and messaging.
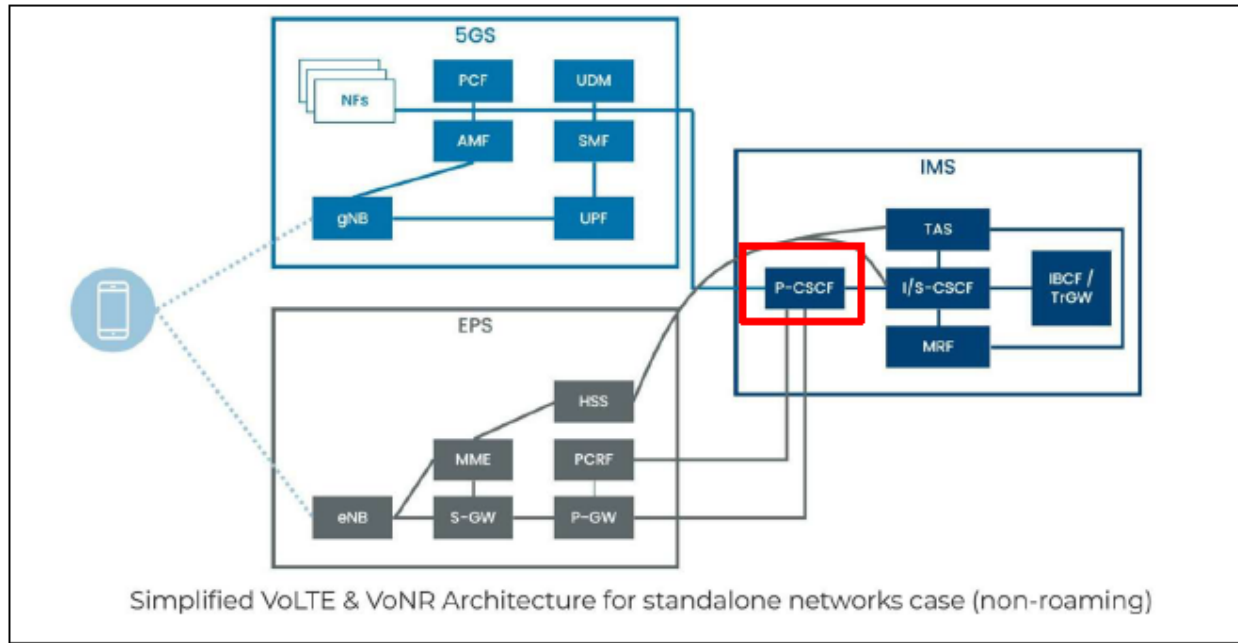
Source: https://www.fierce-network.com/wireless/mavenir-does-many-same-things-ericsson-nokia.

94.   The '789 Accused Products receive "a request to establish a communication session between at least a first communication device associated with a first user and second communication device associated with a second user." For example, the T-Mobile IMS network receives a request to establish a voice call as part of a communication session between a first communication device associated with a first T-Mobile customer and a second communication device associated with a second user:
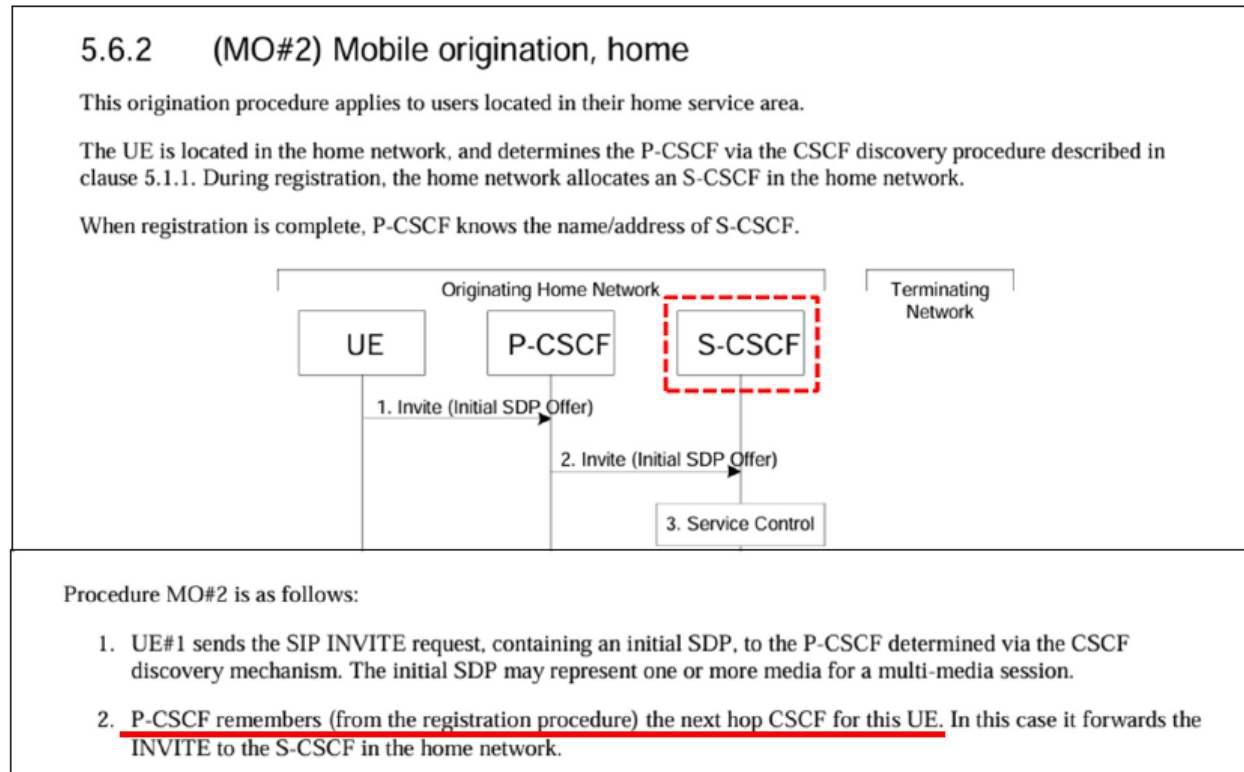

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_123228v140700p.pdf.

T-Mobile IMS network receives a request to establish a voice call as part of a communication session between a first communication device associated with a first T-Mobile customer and a second communication device associated with a second T-Mobile customer:

Simplified VoLTE & VoNR Architecture for standalone networks case (non-roaming)

Source: https://www.3gpp.org/technologies/volte-vonr.

4.6.1   Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs using the mechanism described in the clause "Procedures related to Local CSCF Discovery". The P-CSCF behaves like a Proxy (as defined in IETF RFC 3261 [12] or subsequent versions), i.e. it accepts requests and services them internally or forwards them on. The P-CSCF shall not modify the Request URI in the SIP INVITE message. The P-CSCF may behave as a User Agent (as defined in the IETF RFC 3261 [12] or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

95.   The '789 Accused Products sequence "at least one anchor point in the communication session during set-up of the communication session, wherein the at least one anchor point monitors and controls the communication session for an application to leverage during the communication session and the at least one anchor point server is inserted as a Back-

to-Back User Agent in a signaling path of the communication session." For example, the P-CSCF

will identify the first communication device and determine an S-CSCF that corresponds to the first

communication device:

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_
123228v140700p.pdf.

The S-CSCF performs session control services for the first communication device, including

monitoring the type of communication service requested and subsequently routing the INVITE

message:

4.6.3   Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

- For an originating endpoint (i.e. the originating user/UE, or originating AS)

  - Obtain from a database the Address of the entry point for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and forward the SIP request or response to that entry point.

    If a GRUU is received as the contact, ensures that the Public User Identity of the served user in the request and the Public User Identity encapsulated in the P-GRUU or associated with the T-GRUU belongs to the same service profile.

  - When the destination name of the destination user (e.g. dialled phone number or SIP URI), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.

  - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.

  - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.

  - Ensure the originating end point is subscribed to the determined IMS communication service.

  - Ensure that the content of the SIP request or response (e.g. value included in Content-Type SIP header, media lines included in SDP) sent or received by the originating endpoint matches the determined IMS communication service definition, based on originating user's subscription.

  - When the INVITE message includes an MPS code or an MPS input string, forward the INVITE, including the Service User's priority level if available.

  - When an MPS user is authorized by an AS for priority service, include the Service User's priority level received from the AS in the INVITE and forward the INVITE.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

If an application hosted at an application server is subsequently invoked for the communication session, the S-CSCF will also serve as an anchor point for the application server to leverage in the communication session:

4.2.4b   S-CSCF Service Control Model

Figure 4.3f: Service Control Model with Incoming Leg Control and Outgoing Leg Control

Figure 4.3f illustrates the relationship between the S-CSCF and AS. It includes a first-level of modelling inside the S-CSCF and inside the AS. To keep the model simple only one incoming leg and one outgoing leg are shown. In practice a session may consist of more than one incoming leg and/or more than one outgoing leg(s), when using User Agents. An AS may create one or more outgoing legs independent of incoming legs. An AS may create one or more outgoing legs even when there are no incoming legs.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

The S-CSCF remains an anchor point in the SIP signaling path for the duration of the communication session and follows a proxy back-to-back user agent ("proxy-B2BUA") role. As a proxy-B2BUA, the S-CSCF serves as a pass-through SIP server which can also generate and modify messages on its own:

4.7. S-CSCF Function

The Serving-Call Session Control Function (S-CSCF) is defined by 3GPP [IMS] standards and typically follows a Proxy-B2BUA role.

3.1.1. Proxy-B2BUA

A Proxy-B2BUA is one that appears, from a SIP perspective, to be a SIP proxy based on [RFC3261] and its extensions, except that it maintains a sufficient dialog state to generate in-dialog SIP messages on its own and does so in specific cases. The most common example of this is a SIP proxy that can generate BYE requests to tear down a dead session.

Source: https://datatracker.ietf.org/doc/html/rfc7092.

The S-CSCF remains an anchor point in the SIP signaling path for the duration of the communication session and follows a proxy-B2BUA role. As a proxy-B2BUA, the S-CSCF serves as a pass-through SIP server which can also generate and modify messages on its own:

5.4.5.3   S-CSCF in the Session Path

All initial requests to or from the UE traverse the S-CSCF assigned to the UE. The S-CSCF uses the "Record-Route" mechanism defined in IETF RFC 3261 [12] to remain in the signalling path for subsequent requests too; in short terms: the S-CSCF "record-routes". This is considered the default behaviour for all IMS communication. However, if Application Servers under operator control guarantee the home control of the session, then it may not be required that all subsequent requests traverse the S-CSCF. In such cases the operator may choose that the S-CSCF does not "record-route". The detailed record-route behaviour is configured in the S-CSCF, e.g. on a per-service basis. The S-CSCF decides whether it performs record-routing or not based on operator configuration in the S-CSCF.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

20.30 Record-Route

The Record-Route header field is inserted by proxies in a request to force future requests in the dialog to be routed through the proxy.

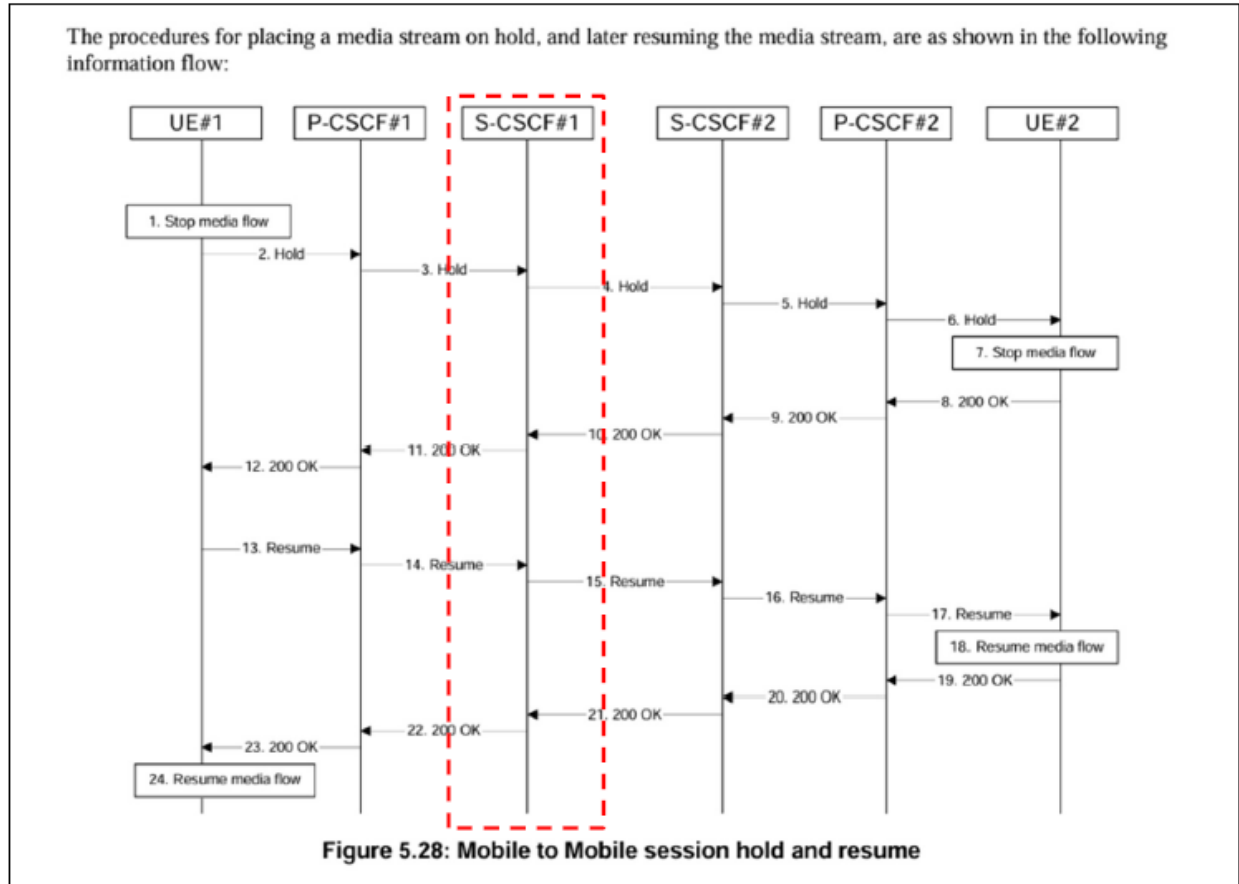Examples of its use with the Route header field are described in Sections 16.12.1.

Source: https://datatracker.ietf.org/doc/rfc3261/.

96.   The '789 Accused Products establish "the communication session and including the anchor point in the signaling path of the communication session." For example, if the second communication device answers the call, a media session is established between the first and second communication devices to facilitate the voice call:

3GPP TS 23.228 version 14.7.0 Release 14	118	ETSI TS 123 228 V14.7.0 (2022-01)

26-27. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end, as specified by the termination procedures and the S-S procedures, to S-CSCF.

28. P-CSCF indicates that the media flows authorized for this session should now be enabled.

29. P-CSCF passes the 200-OK response back to UE

30. UE starts the media flow(s) for this session.

31-33. UE responds to the 200 OK with an ACK message which is sent to P-CSCF and passed along the signalling path to the terminating end.

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_
123228v140700p.pdf.

The S-CSCF remains an anchor point in the signaling path for the duration of the communication session, as evidenced by, for example, the signaling flow for UE #1 placing a call on hold:

The procedures for placing a media stream on hold, and later resuming the media stream, are as shown in the following information flow:

Figure 5.28: Mobile to Mobile session hold and resume

Source: https://www.etsi.org/deliver/etsi_ts/123200_123299/123228/14.07.00_60/ts_ 123228v140700p.pdf.

97.   The '789 Accused Products determine "after the communication session has been established, that a first application which was not initially a part of the communication session is to control at least part of the communication session." For example, compatible T-Mobile phones may add a 3rd caller to the communication session to initiate an ad-hoc conference call:

48

Source: https://www.t-mobile.com/community/discussions/apple/conference-call-with-phone-13-pro/62981.

Applications which provide several services may be invoked, which were not initially part of the communication session (e.g. video calling, conferencing, etc.). For example, if the first user decides to merge calls to create a conference call, the first communication device will send a subsequent INVITE message through the signaling path. The conferencing server will receive the message and determine that the conferencing application which was not initially a part of the communication session will control part of the communication session.

49

Source: https://www.etsi.org/deliver/etsi_ts/124600_124699/124605/18.00.00_60/ts_
124605v180000p.pdf.

If the first user decides to merge calls to create a conference call, the first communication device

will send a subsequent INVITE message through the signaling path. The conferencing server will

receive the message and determine that the conferencing application which was not initially a

part of the communication session will control part of the communication session
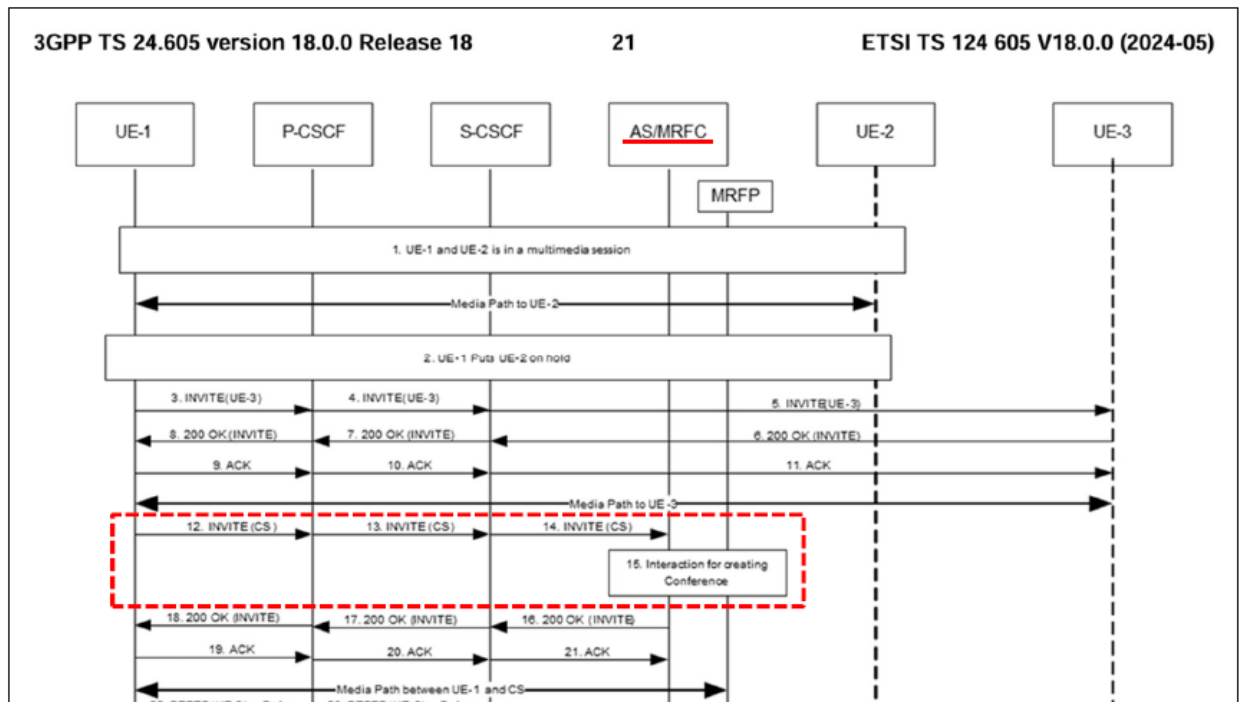
Source: https://www.etsi.org/deliver/etsi_ts/124600_124699/124605/18.00.00_60/ts_
124605v180000p.pdf.

98.   The '789 Accused Products based on the determining step, allow "the at least one

anchor point to serve as a communication session control point for the first application." For

example, the S-CSCF remains in the signaling path for the communication session through the

establishment of the ad-hoc conference, and the S-CSCF serves as an anchor point and sole point

of contact for the T-Mobile conferencing application which now controls part of the media session:
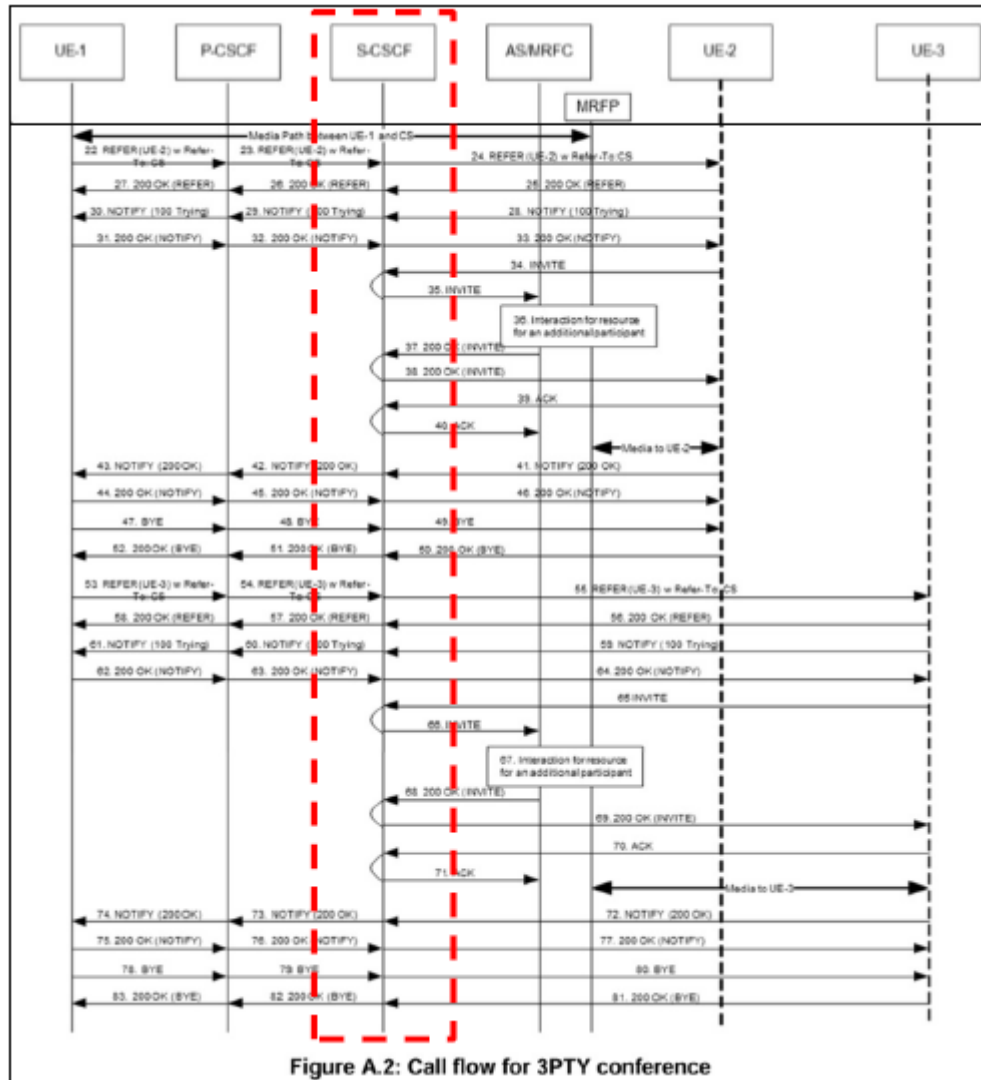
50

Figure A.2: Call flow for 3PTY conference

Source: https://www.etsi.org/deliver/etsi_ts/124600_124699/124605/18.00.00_60/ts_
124605v180000p.pdf.

99.   The technology discussion above and the exemplary '789 Accused Products

provide context for Plaintiff's infringement allegations.

100.   At a minimum, Defendant has known of the '789 patent at least as early as the

service of this complaint. Further, Defendant has known of the '789 patent at least as early as the

filing date of the complaint. In addition, Defendant has known about the '789 patent since at least

receiving correspondence from Plaintiff alerting Defendant to its infringement.

101.   On information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the '789 Accused Products that include or are made using all of the limitations of one or more claims of the '789 patent to directly infringe one or more claims of the '789 patent (e.g., claim 1, as discussed above) by using, offering for sale, selling, and/or importing the '789 Accused Products. Since at least the notice provided on the above-mentioned date, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '789 patent. Defendant intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the '789 Accused Products, creating and/or maintaining established distribution channels for the '789 Accused Products into and within the United States, manufacturing the '789 Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, and testing the '789 Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States. For example, Defendant configures the '789 Accused Products to contain specific instructions, in the form of executable code and configuration files, that cause such products to automatically implement and provide VoLTE as discussed above (i.e., Defendant provides instructions that cause end users to use '789 Accused Products in an infringing manner). Moreover, in addition to the foregoing, Defendant encourages its customers and end users to use VoLTE communications that cause the '789 Accused Products to operate an infringing manner.

102.   In the alternative, on information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '789 patent. For example, Defendant contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the '789 Accused Products. To the extent that the '789 Accused Products do not directly infringe one or more claims of the '789 patent, such products contain instructions, such as source code, that are especially adapted to cause the '789 Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the '789 Accused Products to establish a voice telephone call in an infringing manner and are a material part of the invention of the '789 patent and are not a staple article of commerce suitable for substantial non-infringing use.

103.   On information and belief, despite having knowledge of the '789 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '789 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Defendant's infringing activities relative to the '789 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

104.   Plaintiff has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Plaintiff in an amount that adequately compensates Plaintiff for Defendant's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT V

(INFRINGEMENT OF U.S. PATENT NO. 9,398,055)

105.   Plaintiff incorporates the preceding paragraphs herein by reference.

106.   This cause of action arises under the patent laws of the United States, and, in particular, 35 U.S.C. §§ 271, *et seq*.

107.   Plaintiff is the assignee of the '055 patent, with ownership of all substantial rights in the '055 patent, including the right to exclude others and to enforce, sue, and recover damages for past, present, and future infringements.

108.   The '055 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination.

109.   Defendant has and continues to directly and/or indirectly infringe (by inducing infringement and/or contributing to infringement) one or more claims of the '055 patent in this District and elsewhere in Texas and the United States.

110.   Defendant designs, offers for sale, uses, and sells services, such as its cellular network that includes STIR/SHAKEN call verification ("the '055 Accused Products"), that infringe the '055 patent.

111.   Defendant directly infringes the '055 patent under 35 U.S.C. § 271(a) by using, making, offering for sale, selling, and/or importing the '055 Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '055 patent.

112.   For example, Defendant infringes claim 1 of the '055 patent via the '055 Accused Products. The '055 Accused Products utilize the STIR/SHAKEN standards to verify incoming calls:

NETWORK   PRESS RELEASE

T-Mobile Completes STIR/SHAKEN with ALL Major Carriers to Help Protect Customers from Scams and Spam

March 25, 2021

- **What's the news:** T-Mobile is the first US wireless provider to work with all other major networks – including those with slower 5G networks (which is all of them) – to implement STIR/SHAKEN to fight number spoofing and further protect customers from scammers. With these partnerships, T-Mobile now authenticates calls with wireless and network providers that collectively represent around 98% of wireless customers in the U.S.

Source: https://www.t-mobile.com/news/network/stir-shaken-all-networks.

113.   The '055 Accused Products perform "a secure call indicator method." For example, the '055 Accused Products verify call originators to prevent caller ID spoofing in calls using SIP, on T-Mobile's 4G and 5G networks:

1. Introduction

The Signature-based Handling of Asserted information using toKENs (SHAKEN) [ATIS-1000074] specification defines a framework for using Secure Telephone Identity Revisited (STIR) protocols including PASSporT [RFC8225], SIP Authenticated Identity Management [RFC8224] and the STIR certificate framework [RFC8226] for implementing the cryptographic validation of an authorized originator of telephone calls using SIP. Because the current telephone network contains both VoIP and TDM/SS7 originated traffic, there are many scenarios that need to be accounted for where PASSporT signatures may represent either direct or indirect call origination scenarios. The SHAKEN [ATIS-1000074] specification defines levels of attestation of the origination of the call as well as an origination identifier that can help create a unique association between the origin of a particular call to the point in the VoIP or TDM telephone network the call came from to identify, for example, either a customer or class of service that call represents. This document specifies these values as claims to extend the base set of PASSporT claims.

Source: https://datatracker.ietf.org/doc/html/draft-ietf-stir-passport-shaken-06.

As a part of this process, the T-Mobile IMS network uses Session Initiation Protocol (SIP) for signaling between clients and network nodes to manage 4G and 5G calls serviced by T-Mobile:

IP Multimedia Subsystem (IMS)

Recalling that PS domain came with the limitation that quality of service is more difficult to guarantee than CS domain, supporting voice services over PS domain of 4G (and beyond) networks required due consideration. This is where IP Multimedia Subsystem (IMS) comes in. IMS is defined to be (IMS textbook) "a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end-users using common Internet-based protocols." and is able to provide carrier services over the PS domain data pipe.

The two main protocols of IMS are Session Initiation Protocol (SIP) and Session Description Protocol (SDP). SIP is used to communicate call/session related signalling among the network nodes and the clients and SDP is used to describe the related media of that call/session (e.g. voice media details such as codec etc.). Whilst these protocols are also used by non-carrier Voice over IP (VoIP) services, IMS differs in that the platform interacts closely with the access networks in contrast to typical VoIP services that treat the underlying transport as mere data pipe without guaranteed quality.

Source: https://www.3gpp.org/technologies/volte-vonr.

114.   The '055 Accused Products receive "by a microprocessor, a Session Initiation Protocol ("SIP") message, wherein the SIP message corresponds to a communication session between at least a first communication device associated with a first user and second communication device associated with a second user." For example, the T-Mobile IMS network receives a SIP INVITE message, which corresponds to a communication session between a caller and a T-Mobile customer:

Source: https://datatracker.ietf.org/doc/html/rfc8224/.
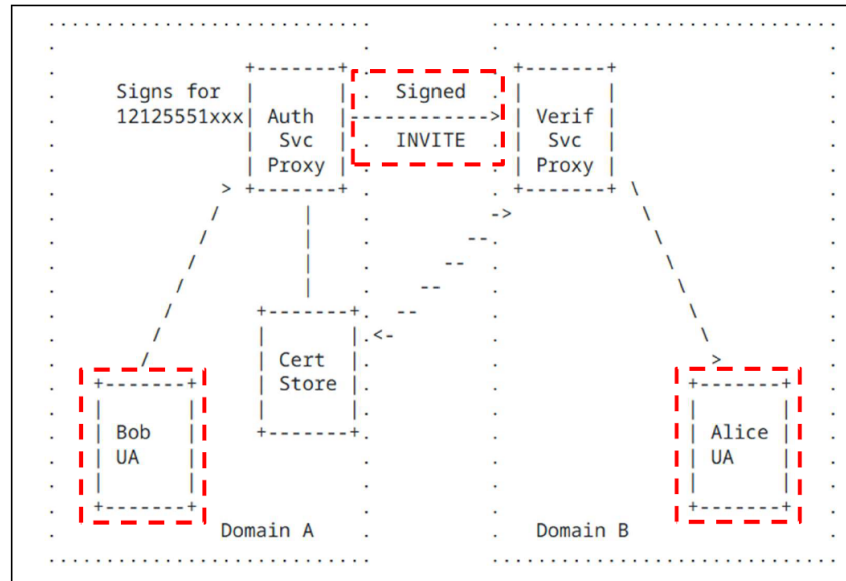
115.   The '055 Accused Products apply "by the microprocessor, a security check to the received SIP message, wherein the security check is for checking trust of a leg of a communication session, wherein the security check inspects each leg of the communication session to determine that each leg of the communication session has passed the security check, and wherein the communication session has a plurality of legs." For example, a security check is applied to the received signed SIP INVITE message, which includes a PASSporT generated by the caller's Authentication Service Proxy, at a Verification Service Proxy within its IMS network:
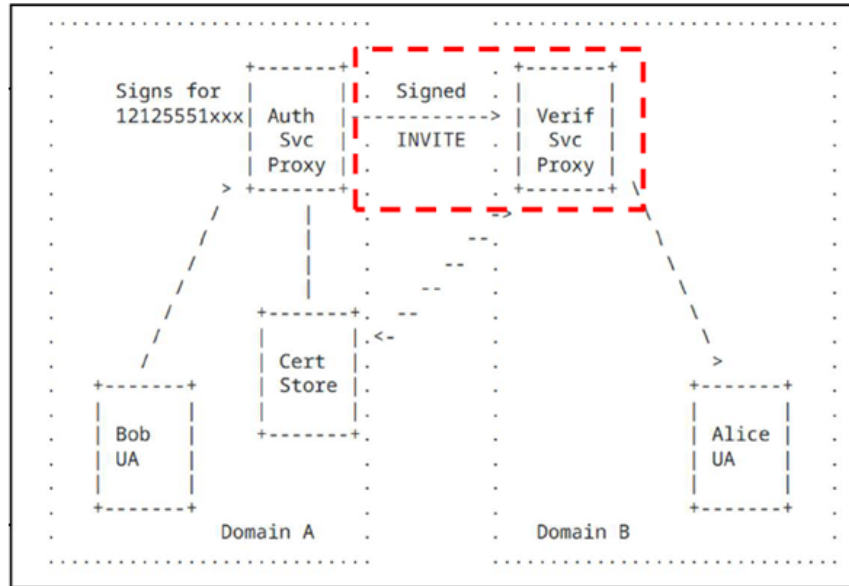


```
5.  Example of Operations

    This section provides an informative (non-normative) high-level
    example of the operation of the mechanisms described in this
    document.

    Imagine a case where Bob, who has the home proxy of example.com and
    the AoR sip:12155551212@example.com;user=phone, wants to communicate
    with Alice at sip:alice@example.com.  They have no prior
    relationship, and Alice implements best practices to prevent
    impersonation attacks.

    Bob's UA generates an INVITE and places his AoR in the From header
    field of the request.  He then sends an INVITE to an authentication
    service proxy for his domain.
```

Source: https://datatracker.ietf.org/doc/html/rfc8224/.

Source: https://datatracker.ietf.org/doc/html/rfc8224/.

The proxy authenticates Bob and validates that he is authorized to assert the identity that he populated in the From header field. The proxy authentication service then constructs a PASSporT that contains a JSON representation of values that mirror certain parts of the SIP request, including the identity in the From header field value. As a part of generating the PASSporT, the authentication service signs a hash of that JSON header and payload with the private key associated with the appropriate credential for the identity (in this example, a certificate with authority to sign for numbers in a range from 12155551000 to 12155551999), and the signature is inserted by the proxy server into the Identity header field value of the request as a compact form of PASSporT. Alternatively, the JSON header and payload themselves might also have been included in the object when using the full form of PASSporT.

The proxy authentication service, as the holder of a private key with authority over Bob's telephone number, is asserting that the originator of this request has been authenticated and that he is authorized to claim the identity that appears in the From header field. The proxy inserts an "info" parameter into the Identity header field that tells Alice how to acquire keying material necessary to validate its credentials (a public key), in case she doesn't already have it.

When Alice's domain receives the request, a proxy verification service validates the signature provided in the Identity header field and then determines that the authentication service credentials demonstrate authority over the identity in the From header field. This same validation operation might be performed by a verification service in Alice's UA server (UAS). Ultimately, this valid request is rendered to Alice. If the validation were unsuccessful, some other treatment could be applied by the receiving domain or Alice's UA.

Source: https://datatracker.ietf.org/doc/html/rfc8224/.

58

```
3.  Overview of "shaken" PASSporT Extension

    The SHAKEN framework is designed to use PASSporT [RFC8225] as a
    method of asserting the caller's telephone identity.  In addition to
    the PASSporT base claims, there are two additional claims that have
    been defined for the needs of a service provider to signal
    information beyond just the telephone identity.  First, in order to
    help bridge the transition of the state of the current telephone
    network (which has calls with no authentication and non-SIP [RFC3261]
    signaling not compatible with the use of PASSporT and Secure
    Telephone Identity (STI) in general), there is an attestation claim.
    This provides three levels of attestation: a full attestation when
    the service provider can fully attest to the calling identity, a
    partial attestation when the service provider originated a telephone
    call but cannot fully attest to the calling identity, and a gateway
    attestation, which is the lowest level of attestation and represents
    the service provider receiving a call from a telephone gateway that
    does not support PASSporT or STI.
```

Source: https://datatracker.ietf.org/doc/rfc8588/.

As part of this process, the INVITE message traverses at least two legs: a Caller Leg from the caller's phone to the authentication service, and an Inter-Network Leg from the authentication service proxy to the Verification Service Proxy:

```
5.  Example of Operations

    This section provides an informative (non-normative) high-level
    example of the operation of the mechanisms described in this
    document.

    Imagine a case where Bob, who has the home proxy of example.com and
    the AoR sip:12155551212@example.com;user=phone, wants to communicate
    with Alice at sip:alice@example.com.  They have no prior
    relationship, and Alice implements best practices to prevent
    impersonation attacks.

    Bob's UA generates an INVITE and places his AoR in the From header
    field of the request.  He then sends an INVITE to an authentication
    service proxy for his domain.
```

```
When Alice's domain receives the request, a proxy verification
service validates the signature provided in the Identity header field
and then determines that the authentication service credentials
demonstrate authority over the identity in the From header field.
This same validation operation might be performed by a verification
service in Alice's UA server (UAS).  Ultimately, this valid request
is rendered to Alice.  If the validation were unsuccessful, some
other treatment could be applied by the receiving domain or
Alice's UA.
```

Source: https://datatracker.ietf.org/doc/html/rfc8224/.
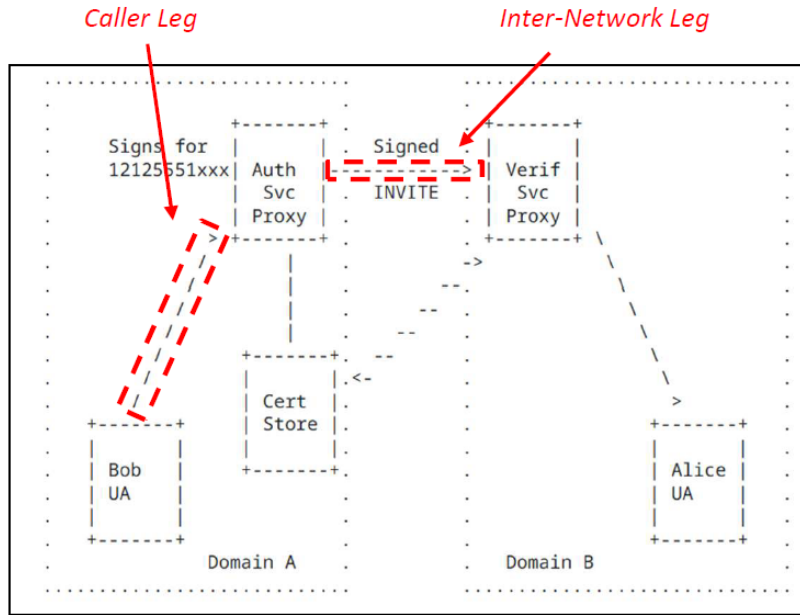
A security check inspects the Caller Leg of the communication session based on the attestation claim in the PASSporT (e.g., determining whether the Caller Leg is secure within the service provider network or includes an unsecured international gateway), thereby assessing the trustworthiness of the Caller Leg to determine if it has passed the security check:

```
4.  PASSporT 'attest' Claim

    This indicator allows for both identifying the service provider that
    is vouching for the call as well as clearly indicating what
    information the service provider is attesting to.  The 'attest' claim
    can be one of the following three values: 'A', 'B', or 'C' as defined
    in [ATIS-1000074].

    'A' represents 'Full Attestation' where the signing provider MUST
    satisfy all of the following conditions:

    o  Is responsible for the origination of the call onto the IP based
       service provider voice network.

    o  Has a direct authenticated relationship with the initiator of the
       call and can identify the customer associated with the initiator.

    o  Has established a verified association with the calling party
       telephone number used for the call.

    'B' represents 'Partial Attestation' where the signing provider MUST
    satisfy all of the following conditions:

    o  Is responsible for the origination of the call onto its IP-based
       voice network.

    o  Has a direct authenticated relationship with the initiator of the
       call and can identify the customer associated with the initiator.

    o  Has NOT established a verified association with the calling party
       telephone number being used for the call.

    'C' represents 'Gateway Attestation' where the signing provider MUST
    satisfy all of the following conditions:

    o  Is the entry point of the call into its VoIP network.

    o  Has no relationship with the initiator of the call (e.g.,
       international gateways)
```

Source: https://datatracker.ietf.org/doc/html/draft-ietf-stir-passport-shaken-06.

A security check also assesses the trust of the Inter-Network Leg by validating the signature in the

PASSporT, which authenticates the authority of the Authentication Service Proxy over the caller

number in the From header field, to determine whether this leg has passed the security check:

The proxy authenticates Bob and validates that he is authorized to assert the identity that he populated in the From header field. The proxy authentication service then constructs a PASSporT that contains a JSON representation of values that mirror certain parts of the SIP request, including the identity in the From header field value. As a part of generating the PASSporT, the authentication service signs a hash of that JSON header and payload with the private key associated with the appropriate credential for the identity (in this example, a certificate with authority to sign for numbers in a range from 12155551000 to 12155551999), and the signature is inserted by the proxy server into the Identity header field value of the request as a compact form of PASSporT. Alternatively, the JSON header and payload themselves might also have been included in the object when using the full form of PASSporT.

The proxy authentication service, as the holder of a private key with authority over Bob's telephone number, is asserting that the originator of this request has been authenticated and that he is authorized to claim the identity that appears in the From header field. The proxy inserts an "info" parameter into the Identity header field that tells Alice how to acquire keying material necessary to validate its credentials (a public key), in case she doesn't already have it.

When Alice's domain receives the request, a proxy verification service validates the signature provided in the Identity header field and then determines that the authentication service credentials demonstrate authority over the identity in the From header field. This same validation operation might be performed by a verification service in Alice's UA server (UAS). Ultimately, this valid request is rendered to Alice. If the validation were unsuccessful, some other treatment could be applied by the receiving domain or Alice's UA.

Source: https://datatracker.ietf.org/doc/html/rfc8224/.

A security check also inspects the leg between the called party's User Agent (UA) and T-Mobile's network, which includes the Verification Service Proxy, by verifying that the called party's UA is authenticated and authorized to be on T-Mobile's network, thereby determining whether this leg has passed the security check:

5.1.2   Authentication and Authorization

The 5G system shall satisfy the following requirements.

Subscription authentication: The serving network shall authenticate the Subscription Permanent Identifier (SUPI) in the process of authentication and key agreement between UE and network.

Serving network authentication: The UE shall authenticate the serving network identifier through implicit key authentication.

    NOTE 1: The meaning of 'implicit key authentication' here is that authentication is provided through the successful use of keys resulting from authentication and key agreement in subsequent procedures.

    NOTE 2: The preceding requirement does not imply that the UE authenticates a particular entity, e.g. an AMF, within a serving network.

UE authorization: The serving network shall authorize the UE through the subscription profile obtained from the home network. UE authorization is based on the authenticated SUPI.

Source: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/18.08.00_60/ts_133501v 180800p.pdf.

> **Primary authentication**: Network and device mutual authentication in 5G is based on primary authentication. This is similar to 4G but there are a few differences. The authentication mechanism has in-built home control allowing the home operator to know whether the device is authenticated in a given network and to take final call of authentication. In 5G Phase 1 there are two mandatory authentication options: 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol (EAP)-AKA', i.e. EAP-AKA'. Optionally, other EAP based authentication mechanisms are also allowed in 5G - for specific cases such as private networks. Also, primary authentication is radio access technology independent, thus it can run over non-3GPP technology such as IEEE 802.11 WLANs.

Source: https://www.3gpp.org/news-events/3gpp-news/sec-5g.

> In Rel-15, SA3 specified that EAP-AKA' is, besides 5G-AKA, one of the two mandatory authentication methods for accessing the 5G core network via any access type. This integrates the EAP framework firmly into 5G security, compared to EPS where EAP-AKA/EAP-AKA' support was used only for the non-3GPP access type. The authentication framework for 5G and the usage of EAP-AKA' for authentication to 5G networks is described in clause 6.1 of TS 33.501 [m].

Source: https://www.3gpp.org/technologies/sec-npn.

116.   The '055 Accused Products determine "by the microprocessor, based on the security check, a security classification associated with the communication session." For example, the Accused Products assign a security classification to the received call, associated with the communication session, based on the security check, such as "Scam Likely," "Telemarketing," or "Nuisance." Calls identified as spoofed, based on the SHAKEN security check, are classified as

"Scam Likely." Conversely, incoming calls that pass the security check and show no other signs of being a scam or unwanted solicitation are classified as "Number Verified."

Scam ID & Scam Block

Scam ID and Scam Block are industry-leading free scam protection tools deployed on the T-Mobile network to keep our customers safe from scammers.

- Scam ID automatically displays "Scam Likely" and the number that is calling on suspected scam calls
- As an additional network level identification feature, customers will also see some calls labeled as Telemarketing, Political, Nuisance etc. These are automatically identified at T-Mobile's network level and displayed to our subscribers to help them in making informed decisions on which calls they would like to interact with.
- Scam ID also catches spoofed calls because T-Mobile reviews beyond the incoming number and tracks actual call behavior.
- Scam Block automatically blocks all "Scam Likely" calls before they ever reach your phone, so you never even get them.
- Network-level protection has been added to stop the increasingly common "Neighborhood Spoofing" and prevent hijacked numbers (where scammers temporarily match the area code and 3-digit prefix of the person they are targeting) from reaching your phone.
- The free website **https://www.freecallerregistry.com/fcr/** gives businesses the ability to register their business number(s) and name, so their calls to customers are recognized as legitimate.

Source: https://www.t-mobile.com/support/plans-features/help-with-scams-spam-and-fraud.

- **What's the news:** T-Mobile is the first US wireless provider to work with all other major networks – including those with slower 5G networks (which is all of them) – to implement STIR/SHAKEN to fight number spoofing and further protect customers from scammers. With these partnerships, T-Mobile now authenticates calls with wireless and network providers that collectively represent around 98% of wireless customers in the U.S.
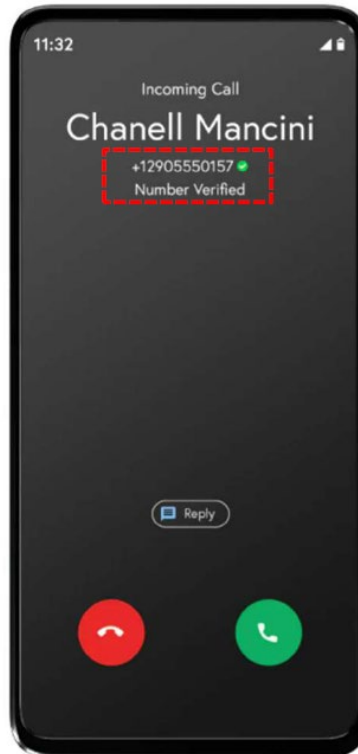
Source: https://www.t-mobile.com/news/network/stir-shaken-all-networks.

What is Scam Likely?

When our network filters detect a potential scam call, we flag it and display it as Scam Likely on your device. This is made possible by our Scam ID technology which is embedded in our network and is enabled by default for all T-Mobile customers. No action is required on the part of customers to enable it, and it's free.

Source: https://www.t-mobile.com/benefits/scam-shield.

117.   The '055 Accused Products control "by the microprocessor, a secure call indicator on one of the second communication device associated with the second user or the at least one first communication device associated with the first user, wherein the secure call indicator indicates the security classification associated with the communication session, and wherein the security

classification indicates to the one of the first or second user whether the communication session is secure or unsecure. For example, the '055 Accused Products control a secure call indicator on the T-Mobile customer's device to indicate the security classification of the communication session, the security classification being one of at least "Number Verified", "Telemarketing", and "Scam Likely":

Source: https://www.t-mobile.com/news/press/t-mobile-calls-are-100-stir-shaken-compliant.

Scam block.

Stop scammers before you take the call by turning on Scam Block. Keep track of scam calls you've blocked or received with the Scam Counter.
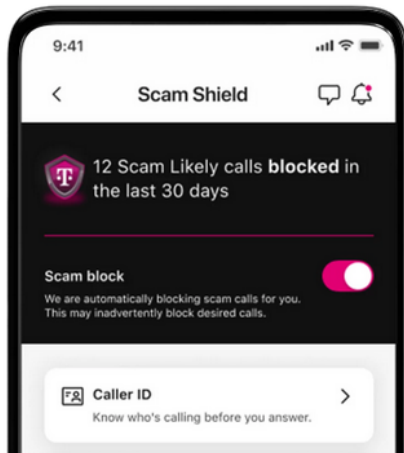
Caller ID.

Reduce unidentified calls by displaying a caller's information, even if they're not in your contact list. You can also see if a call is in a spam category such as telemarketing.

Source: https://www.t-mobile.com/benefits/scam-shield.

What is Scam Likely?

When our network filters detect a potential scam call, we flag it and display it as Scam Likely on your device. This is made possible by our Scam ID technology which is embedded in our network and is enabled by default for all T-Mobile customers. No action is required on the part of customers to enable it, and it's free.

Source: https://www.t-mobile.com/benefits/scam-shield.

118.   The technology discussion above and the exemplary '055 Accused Products provide context for Plaintiff's infringement allegations.

119.   At a minimum, Defendant has known of the '055 patent at least as early as the service of this complaint. Further, Defendant has known of the '055 patent at least as early as the filing date of the complaint. In addition, Defendant has known about the '055 patent since at least receiving correspondence from Plaintiff alerting Defendant to its infringement.

120.   On information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has actively induced, under U.S.C. § 271(b), its

distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the '055 Accused Products that include or are made using all of the limitations of one or more claims of the '055 patent to directly infringe one or more claims of the '055 patent (e.g., claim 1, as discussed above) by using, offering for sale, selling, and/or importing the '055 Accused Products. Since at least the notice provided on the above-mentioned date, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '055 patent. Defendant intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the '055 Accused Products, creating and/or maintaining established distribution channels for the '055 Accused Products into and within the United States, manufacturing the '055 Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, and testing the '055 Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States. For example, Defendant configures the '055 Accused Products to contain specific instructions, in the form of executable code and configuration files, that cause such products to automatically implement and provide STIR/SHAKEN call verification as discussed above (i.e., Defendant provides instructions that cause end users to use '055 Accused Products in an infringing manner). Moreover, in addition to the foregoing, Defendant encourages its customers and end users to use STIR/SHAKEN call verification that causes the '055 Accused Products to operate an infringing manner.

121.   In the alternative, on information and belief, since at least the above-mentioned date when Defendant was on notice of its infringement, Defendant has contributorily infringed, under

U.S.C. § 271(c), one or more claims of the '055 patent. For example, Defendant contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the '055 Accused Products. To the extent that the '055 Accused Products do not directly infringe one or more claims of the '055 patent, such products contain instructions, such as source code, that are especially adapted to cause the '055 Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the '055 Accused Products to provide STIR/SHAKEN call verification in an infringing manner and are a material part of the invention of the '055 patent and are not a staple article of commerce suitable for substantial non-infringing use.

122.   On information and belief, despite having knowledge of the '055 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '055 patent, Defendant has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Defendant's infringing activities relative to the '055 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

123.   Plaintiff has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Plaintiff in an amount that adequately compensates Plaintiff for Defendant's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

124.   Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's wrongful acts, and willful infringement, in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

125.   Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

126.   Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

127.   Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

i.   A judgment that Defendant has infringed the Asserted Patents as alleged herein, directly and/or indirectly, by way of by way of inducement and/or contributory infringement of such patents;

ii.   A judgment for an accounting of all damages sustained by Plaintiff as a result of the acts of infringement by Defendant;

iii.   A judgment and order requiring Defendant to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;

iv.   A judgment and order requiring Defendant to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

v.   A judgment and order finding this to be an exceptional case and requiring Defendant to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and

vi.   Such other and further relief as the Court deems just and equitable.

Dated: March 7, 2025

Respectfully submitted,

/s/ *Patrick J. Conroy*
Patrick J. Conroy (Lead Counsel)
Texas Bar No. 24012448
Justin B. Kimble
Texas Bar No. 24036909
Jon Rastegar
Texas Bar No. 24064043
Nathan L. Levenson
Texas Bar No. 24097992
Nelson Bumgardner Conroy PC
2727 N. Harwood St.
Suite 250
Dallas, TX 75201
Tel: (817) 377-9111
pat@nelbum.com
justin@nelbum.com
jon@nelbum.com
nathan@nelbum.com

Attorneys for Plaintiff
Arlington Technologies LLC